Guia GuardDuty do usuário da Amazon

Amazon GuardDuty



Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon GuardDuty: Guia GuardDuty do usuário da Amazon

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

As marcas comerciais e imagens de marcas da Amazon não podem ser usadas no contexto de nenhum produto ou serviço que não seja da Amazon, nem de qualquer maneira que possa gerar confusão entre os clientes ou que deprecie ou desprestigie a Amazon. Todas as outras marcas comerciais que não pertencem à Amazon pertencem a seus respectivos proprietários, que podem ou não ser afiliados, patrocinados pela Amazon ou ter conexão com ela.

Table of Contents

O que é GuardDuty? 1
Características do GuardDuty 2
Compatibilidade com PCI DSS 7
Preços em GuardDuty 8
Usando o GuardDuty teste gratuito de 30 dias 8
Usando a proteção contra malware para S3 com nível gratuito 10
Acessando GuardDuty 10
Conceitos e termos-chave 12
Introdução 18
Antes de começar 18
Etapa 1: habilitar a Amazon GuardDuty 20
Etapa 2: gerar descobertas de amostra e explorar as operações básicas 22
Etapa 3: Configurar a exportação de GuardDuty descobertas para um bucket do Amazon S3 24
Etapa 4: configurar alertas de GuardDuty busca por meio do SNS 29
Próximas etapas 33
Fontes de dados fundamentais 34
AWS CloudTrail eventos de gerenciamento 34
Como GuardDuty manuseia AWS CloudTrail eventos globais 35
Logs de fluxo da VPC 36
Logs de consultas de DNS do Route53 Resolver 37
Detecção de Ameaças Avançada 38
Exemplos de cenários de ameaças com sequência de ataque 38
Como funciona a Detecção de Ameaças Avançada 39
Habilitação de planos de proteção para maximizar a detecção de ameaças 40
Detecção de sequências de ataque em clusters do Amazon EKS 41
Detecção de sequências de ataque nos buckets do Amazon S3 42
Detecção de sequências de ataque em clusters do Amazon ECS 43
Detecção de sequências de ataque em grupos de instâncias do Amazon EC2 44
Detecção de sequências de ataque envolvendo cargas de trabalho de IA 44
Detecção estendida de ameaças no GuardDuty console 45
Noções básicas e gerenciamento de descobertas de sequências de ataques 46
Recursos adicionais do 46
Planos de proteção 47
Visão geral do 47

Configurando todos os planos de proteção ... 48
Auto-enable opções ... 48
Configuração de monitoramento de tempo de execução ... 49
Restrições bidirecionais ... 49
Estatísticas da organização ... 50
Integração da página de contas ... 50
Proteção da IA ... 51
Como funciona a proteção de IA ... 52
Preços da proteção de IA ... 53
Detecções adicionais de ameaças para cargas de trabalho de IA ... 54
Habilitando a proteção de IA em ambientes com várias contas ... 54
Ativando o AI Protection para uma conta independente ... 58
Proteção do EKS ... 60
Logs de auditoria do EKS na Proteção EKS ... 61
Habilitando a Proteção do EKS em ambientes de várias contas ... 62
Ativando a Proteção do EKS para uma conta independente ... 69
Proteção do S3 ... 71
AWS CloudTrail eventos de dados para S3 ... 72
Como GuardDuty usa eventos CloudTrail de dados para o S3 ... 72
GuardDuty usando eventos CloudTrail de dados para S3 para sequências de ataque ... 73
Habilitando a Proteção do S3 em ambientes de várias contas ... 73
Ativando a Proteção do S3 para uma conta independente ... 81
Monitoramento de runtime ... 83
Como funcionam ... 84
Capacitação ... 85
Implante no Amazon EKS ... 86
Implemente no Amazon EC2 ... 88
Implante no Amazon ECS no Fargate ... 90
Conectividade do agente ... 91
Rastreando a cobertura do monitoramento do ... 93
Avaliação gratuita de 30 dias ... 94
Estou usando o período de GuardDuty teste ou nunca habilitei o EKS Runtime Monitoring ... 94
Eu habilitei o Monitoramento de runtime do EKS antes do lançamento do Monitoramento de runtime ... 95
Pré-requisitos ... 96
Para uma instância do EC2 ... 96

Para ECS-EC2 Bottlerocket 100
Para cluster Fargate (somente ECS) 104
Para cluster do EKS 110
Arquiteturas de CPU, sistemas operacionais e versões do kernel compatíveis 113
Como habilitar o monitoramento de runtime 115
Habilitando o Monitoramento de runtime do EKS para ambientes com várias contas 116
Habilitando o Monitoramento de runtime para uma conta autônoma 119
Gerenciando agentes GuardDuty de segurança 119
Atendente automatizado no recurso Amazon EC2 120
Gerenciamento manual de agente para o Amazon EC2 133
Agente automatizado no recurso ECS-EC2 Bottlerocket 149
Agente automatizado no recurso Fargate (somente Amazon ECS) 151
Atendente automatizado no recurso Amazon EKS 187
Gerenciamento manual de agente para o cluster Amazon EKS 224
Configurar parâmetros do complemento do EKS 233
Validando a configuração do endpoint da VPC 236
Problemas de cobertura de runtime e solução de problemas 238
Cobertura e solução de problemas para recursos do Amazon EC2 239
Cobertura e solução de problemas para ECS-EC2 Bottlerocket 256
Cobertura e solução de problemas para clusters do Amazon ECS 264
Cobertura e solução de problemas para clusters do Amazon EKS 281
Configurar o monitoramento da CPU e da memória 297
Como usar uma VPC compartilhada 298
Como funciona 299
Pré-requisitos 301
Como usar o IaC com agentes automatizados 302
Visão geral do gráfico de dependência de recursos da IaC 302
Problema comum - Como excluir recursos na IaC 302
Tipos de eventos de runtime coletados 304
Eventos do processo 304
Eventos de contêineres 306
AWS Fargate Eventos de tarefas (somente Amazon ECS) 307
Eventos de pod do Kubernetes 308
Eventos do Sistema de Nomes de Domínio (DNS) 308
Eventos abertos 309
Evento do módulo de carga 310

Eventos do Mprotect 310
Eventos de montagem 310
Eventos de links 311
Eventos do Symlink 311
Eventos Dup 312
Evento do mapa de memória 312
Eventos de soquete 313
Eventos de conexão 313
Processar eventos Readv da VM 314
Processar eventos Writev da VM 315
Eventos de rastreio de processo (Ptrace) 315
Vincular eventos 316
Eventos de escuta 317
Eventos de renomeação 317
Eventos Definir ID de usuário (UID) 318
Eventos Chmod 318
Agente de hospedagem de repositórios Amazon ECR GuardDuty 318
Repositório ECR para EKS v1.16.0 - 1.8.1 (eks.build.2) 319
Repositório do ECR para versão do EKS `1.8.1.eks.build.1` 324
Repositório ECR para agente de segurança ativado (somente AWS Fargate Amazon ECS) 327
Repositório ECR para agente de segurança no Bottlerocket ECS-EC2 331
Atendentes de segurança no mesmo host 335
Visão geral do 335
Impacto 335
Como GuardDuty lida com vários agentes 335
Monitoramento de runtime do EKS 336
Configuração do Monitoramento de runtime do EKS para ambientes com várias contas (API) 337
Configuração do Monitoramento de runtime do EKS para uma conta autônoma (API) 379
Migração do Monitoramento de runtime do EKS para o Monitoramento de runtime 386
GuardDuty versões de lançamento do agente de segurança 390
Recursos adicionais – próximas etapas 435
Desativação, desinstalação e remoção de recursos 435
Desinstalação manual do agente de segurança para recursos do Amazon EC2 437
Desinstalando o agente de segurança para recursos do ECS-EC2 Bottlerocket 439

Como remover os recursos do agente de segurança 440
Proteção contra malware para o EC2 442
Comparando a verificação de GuardDuty-initiated malware e a verificação de On-demand malware 443
Como GuardDuty escaneia volumes do EBS em busca de detecção de malware 446
Volumes do EBS compatíveis 447
Modificar o ID da chave KMS padrão 448
Configurar a retenção de snapshots e a cobertura de verificação do EC2 449
Retenção de snapshots 450
Opções de verificação com tags definidas pelo usuário 451
Tag `GuardDutyExcluded` global 455
GuardDuty-initiated escaneamento de malware 455
Avaliação gratuita de 30 dias 457
Habilitando a verificação de GuardDuty-initiated malware em ambientes com várias contas 458
Ativando a verificação de GuardDuty-initiated malware para uma conta independente 468
Descobertas que invocam a verificação de GuardDuty-initiated malware 469
On-demand escaneamento de malware 472
Como funciona a verificação de On-demand malware 473
Iniciando a verificação de On-demand malware 474
Re-scanning instância do Amazon EC2 escaneada anteriormente 477
Monitoramento de status e resultados de verificação de malware 477
GuardDuty conta de serviço 479
Cotas na Proteção contra malware para o EC2 482
Proteção contra malware para S3 487
Preço e custo de uso 489
Analisando o custo de uso 490
Como funciona 491
Visão geral do 491
Permissões de perfil do IAM 491
Criação opcional de tags de objetos com base no resultado da verificação 491
Processe depois de habilitar a Proteção contra malware para o S3 para um bucket 492
Capacidades da proteção contra malware para S3 494
(Opcional) Comece a usar Proteção contra Malware para S3 do GuardDuty de forma independente (somente console) 496
Configurando a proteção contra malware para S3 para seu bucket 497

Habilitando a proteção contra malware para detecção de ameaças do S3 para seu bucket . 498
Permissões de perfil do IAM 504
Solução de problemas de erro de permissões de perfil do IAM 510
Etapas para habilitar a proteção contra malware para S3 511
On-demand Análise de malware S3 512
Pré-requisitos 512
Inicie a verificação de malware sob demanda 513
Usando controle de acesso baseado em tags (TBAC) 513
Adicionando TBAC ao recurso do bucket do S3 514
Visualizar e entender o status do bucket protegido 516
Monitoramento de verificações de objetos de S3 518
Status de verificação potencial do objeto S3 e status do resultado 518
Usando a Amazon EventBridge 522
Uso de marcações de objeto S3 532
Usando CloudWatch alarmes e métricas 533
Solução de problemas 537
Solução de problemas do status do plano de proteção contra malware 537
Solução de problemas de escaneamento de malware sob demanda 541
Editando o plano de proteção contra malware para um bucket protegido 541
Desativando a proteção contra malware para S3 em um bucket protegido 543
Suportabilidade dos atributos do Amazon S3 545
Cotas de Proteção contra malware para o S3 553
Proteção contra malware para AWS backup 556
Visão geral do 556
Como funciona 559
Visão geral do 556
Função do IAM necessária para digitalização 561
Analisando o status e o resultado do escaneamento de recursos 561
Revisar descobertas geradas 561
Permissões de função do IAM 562
Função de cliente fornecida para verificação de malware 562
Detalhes sobre as permissões 563
Protegendo a função 564
Como a Proteção contra GuardDuty Malware usa subsídios em AWS KMS 564
GuardDuty Contexto de criptografia de proteção contra malware 565
Política de permissões e confiança para a função 566

Comece de forma independente ... 570
Etapas para começar a usar o Malware Protection for Backup ... 570
Iniciando varreduras sob demanda ... 571
Console ... 571
API/CLI ... 572
Monitoramento de status e resultados de verificação de malware ... 572
Proteção contra malware para cotas de backup ... 581
Proteção do RDS ... 587
Bancos de dados compatíveis ... 589
Atividade de login do RDS ... 590
Atividade de dados do RDS ... 591
Como habilitar a Proteção do RDS em ambientes com várias contas ... 592
Como habilitar a Proteção do RDS para uma conta autônoma ... 600
Solução de problemas de monitoramento da Proteção do RDS ... 602
Armazenamento do RDS cheio ... 602
Versões não compatíveis no banco de dados primário do RDS for PostgreSQL ... 603
Considerações adicionais sobre segurança ... 603
Proteção do Lambda ... 604
Monitoramento de atividades da rede Lambda ... 605
Como habilitar a proteção Lambda em ambientes com várias contas ... 605
Como habilitar a Proteção Lambda para uma conta autônoma ... 613
Investigação - Pré-visualização ... 615
Tipos de análise ... 615
Cross-Region inferência ... 616
Pré-requisitos ... 617
Modelo de acesso para contas de administrador e membro ... 618
Criando uma investigação ... 619
Visualizando os resultados da investigação ... 621
Interpretação dos resultados da investigação ... 623
Listando investigações ... 624
Regras de detecção personalizadas ... 627
Como funcionam as regras de detecção personalizadas ... 628
Fontes de dados e sinais ... 628
Modos ... 629
Encontrando agregação ... 630
Campos de eventos editados ... 630

Regras de detecção personalizadas disponíveis 631
Visualizando a lógica de detecção de regras 632
Funções usadas na lógica de detecção 633
Gerenciando regras de detecção personalizadas 635
Listando as regras disponíveis 635
Visualizando o status da regra 636
Operações em massa 636
Corrida a seco 637
Ao vivo 638
Desativando regras 639
Gerenciando regras de detecção personalizadas em ambientes com várias contas 639
Configurações da organização 640
Executando os dois modos para a mesma regra 641
Exemplo: aplicar uma regra no modo dry run a todas as contas dos membros 642
Aplicando todas as regras em uma organização 642
Gerenciar várias contas 643
Relações entre administradores do Macie e contas de membros 644
Status do relacionamento do membro 648
Como gerenciar contas com o AWS Organizations 650
Considerações e recomendações 651
Permissões necessárias para designar uma conta de administrador delegado GuardDuty .. 653
Designando uma conta de administrador delegado GuardDuty 654
Como configurar as preferências de habilitação automática da organização 656
Como adicionar membros à organização 660
(Opcional) Ativar planos de proteção para contas-membro existentes 662
Gerenciando continuamente suas contas de membros em GuardDuty 663
Suspensão da GuardDuty conta de membro 664
Como desassociar (remover) a conta-membro da conta de administrador 666
Excluindo contas de membros da organização GuardDuty 667
Alterando a conta do GuardDuty administrador delegado 669
Gerenciando contas usando as políticas da organização 671
Pré-requisitos 672
Como as políticas da organização funcionam 672
Criação de uma política no console 675
Analisar o impacto de uma política antes de aplicá-la 676
Considerações e limitações 677

Gerenciar contas por convite 680
Adição de contas por convite 681
Consolidação de contas de administrador em uma única organização 686
GuardDuty considerações sobre a opção Exportar CSV em contas 689
Tipos de descoberta 690
Tipos de descoberta do EC2 690
Backdoor:EC2/C&CActivity.B 692
Backdoor:EC2/C&CActivity.B!DNS 693
Backdoor:EC2/DenialOfService.Dns 694
Backdoor:EC2/DenialOfService.Tcp 695
Backdoor:EC2/DenialOfService.Udp 695
Backdoor:EC2/DenialOfService.UdpOnTcpPorts 696
Backdoor:EC2/DenialOfService.UnusualProtocol 697
Backdoor:EC2/Spambot 697
Behavior:EC2/NetworkPortUnusual 698
Behavior:EC2/TrafficVolumeUnusual 698
CryptoCurrency:EC2/BitcoinTool.B 699
CryptoCurrency:EC2/BitcoinTool.B!DNS 700
DefenseEvasion:EC2/UnusualDNSResolver 700
DefenseEvasion:EC2/UnusualDoHActivity 701
DefenseEvasion:EC2/UnusualDoTActivity 701
Impact:EC2/AbusedDomainRequest.Reputation 702
Impact:EC2/BitcoinDomainRequest.Reputation 703
Impact:EC2/MaliciousDomainRequest.Reputation 703
Impact:EC2/MaliciousDomainRequest.Custom 704
Impact:EC2/PortSweep 705
Impact:EC2/SuspiciousDomainRequest.Reputation 705
Impact:EC2/WinRMBruteForce 706
Recon:EC2/PortProbeEMRUnprotectedPort 706
Recon:EC2/PortProbeUnprotectedPort 707
Recon:EC2/Portscan 708
Trojan:EC2/BlackholeTraffic 709
Trojan:EC2/BlackholeTraffic!DNS 709
Trojan:EC2/DGADomainRequest.B 710
Trojan:EC2/DGADomainRequest.C!DNS 711
Trojan:EC2/DNSDataExfiltration 712

Trojan:EC2/DriveBySourceTraffic!DNS 712
Trojan:EC2/DropPoint 713
Trojan:EC2/DropPoint!DNS 713
Trojan:EC2/PhishingDomainRequest!DNS 714
UnauthorizedAccess:EC2/MaliciousIPCaller.Custom 714
UnauthorizedAccess:EC2/MetadataDNSRebind 715
UnauthorizedAccess:EC2/RDPBruteForce 716
UnauthorizedAccess:EC2/SSHBruteForce 717
UnauthorizedAccess:EC2/TorClient 718
UnauthorizedAccess:EC2/TorRelay 719
Tipos de descobertas do IAM 719
CredentialAccess:IAMUser/AnomalousBehavior 721
CredentialAccess:IAMUser/CompromisedCredentials 721
DefenseEvasion:IAMUser/AnomalousBehavior 722
DefenseEvasion:IAMUser/BedrockLoggingDisabled 723
Discovery:IAMUser/AnomalousBehavior 723
Exfiltration:IAMUser/AnomalousBehavior 724
Impact:IAMUser/AnomalousBehavior 725
InitialAccess:IAMUser/AnomalousBehavior 725
PenTest:IAMUser/KaliLinux 726
PenTest:IAMUser/ParrotLinux 727
PenTest:IAMUser/PentooLinux 727
Persistence:IAMUser/AnomalousBehavior 728
Policy:IAMUser/RootCredentialUsage 728
Policy:IAMUser/ShortTermRootCredentialUsage 729
PrivilegeEscalation:IAMUser/AnomalousBehavior 730
Recon:IAMUser/MaliciousIPCaller 731
Recon:IAMUser/MaliciousIPCaller.Custom 731
Recon:IAMUser/TorIPCaller 732
Stealth:IAMUser/CloudTrailLoggingDisabled 732
Stealth:IAMUser/PasswordPolicyChange 733
UnauthorizedAccess:IAMUser/ConsoleLoginSuccess.B 733
UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.InsideAWS 734
UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS 736
UnauthorizedAccess:IAMUser/MaliciousIPCaller 737
UnauthorizedAccess:IAMUser/MaliciousIPCaller.Custom 738

UnauthorizedAccess:IAMUser/ResourceCredentialExfiltration.InsideAWS 738
UnauthorizedAccess:IAMUser/ResourceCredentialExfiltration.OutsideAWS 740
UnauthorizedAccess:IAMUser/TorIPCaller 742
Tipos de descoberta de sequência de ataque 742
AttackSequence:EKS/CompromisedCluster 743
AttackSequence:ECS/CompromisedCluster 744
AttackSequence:EC2/CompromisedInstanceGroup 745
AttackSequence:IAM/CompromisedCredentials 746
AttackSequence:S3/CompromisedData 747
Tipos de localização de regras de detecção personalizadas 747
Regras de detecção personalizadas para AWS CloudTrail eventos de gerenciamento 748
Regras de detecção personalizadas para monitoramento de tempo de execução 753
Tipos de descoberta da Proteção do S3 758
Discovery:S3/AnomalousBehavior 760
Discovery:S3/MaliciousIPCaller 760
Discovery:S3/MaliciousIPCaller.Custom 761
Discovery:S3/TorIPCaller 761
Exfiltration:S3/AnomalousBehavior 762
Exfiltration:S3/MaliciousIPCaller 763
Impact:S3/AnomalousBehavior.Delete 763
Impact:S3/AnomalousBehavior.Permission 764
Impact:S3/AnomalousBehavior.Write 765
Impact:S3/MaliciousIPCaller 766
PenTest:S3/KaliLinux 766
PenTest:S3/ParrotLinux 767
PenTest:S3/PentooLinux 767
Policy:S3/AccountBlockPublicAccessDisabled 768
Policy:S3/BucketAnonymousAccessGranted 768
Policy:S3/BucketBlockPublicAccessDisabled 769
Policy:S3/BucketPublicAccessGranted 770
Stealth:S3/ServerAccessLoggingDisabled 771
UnauthorizedAccess:S3/MaliciousIPCaller.Custom 771
UnauthorizedAccess:S3/TorIPCaller 772
Tipos de descoberta da Proteção do EKS 772
CredentialAccess:Kubernetes/MaliciousIPCaller 774
CredentialAccess:Kubernetes/MaliciousIPCaller.Custom 775

CredentialAccess:Kubernetes/SuccessfulAnonymousAccess 776
CredentialAccess:Kubernetes/TorIPCaller 776
DefenseEvasion:Kubernetes/MaliciousIPCaller 777
DefenseEvasion:Kubernetes/MaliciousIPCaller.Custom 778
DefenseEvasion:Kubernetes/SuccessfulAnonymousAccess 778
DefenseEvasion:Kubernetes/TorIPCaller 779
Discovery:Kubernetes/MaliciousIPCaller 780
Discovery:Kubernetes/MaliciousIPCaller.Custom 780
Discovery:Kubernetes/SuccessfulAnonymousAccess 781
Discovery:Kubernetes/TorIPCaller 782
Execution:Kubernetes/ExecInKubeSystemPod 783
Impact:Kubernetes/MaliciousIPCaller 783
Impact:Kubernetes/MaliciousIPCaller.Custom 784
Impact:Kubernetes/SuccessfulAnonymousAccess 784
Impact:Kubernetes/TorIPCaller 785
Persistence:Kubernetes/MaliciousIPCaller 786
Persistence:Kubernetes/MaliciousIPCaller.Custom 786
Persistence:Kubernetes/SuccessfulAnonymousAccess 787
Persistence:Kubernetes/TorIPCaller 788
Policy:Kubernetes/AdminAccessToDefaultServiceAccount 788
Policy:Kubernetes/AnonymousAccessGranted 789
Policy:Kubernetes/ExposedDashboard 790
Policy:Kubernetes/KubeflowDashboardExposed 790
CredentialAccess:Kubernetes/AnomalousBehavior.SecretsAccessed 791
PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleBindingCreated 792
Execution:Kubernetes/AnomalousBehavior.ExecInPod 793
PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!PrivilegedContainer 793
Persistence:Kubernetes/AnomalousBehavior.WorkloadDeployed!ContainerWithSensitiveMount 794
Execution:Kubernetes/AnomalousBehavior.WorkloadDeployed 795
PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleCreated 797
Discovery:Kubernetes/AnomalousBehavior.PermissionChecked 798
Tipos de descoberta do Monitoramento de runtime 798
Encontrando tipos que o Runtime Monitoring gera por padrão 799
Encontrando tipos que exigem regras de detecção personalizadas 837

Tipos de descoberta da Proteção contra malware para EC2 839
Execution:EC2/MaliciousFile 840
Execution:ECS/MaliciousFile 841
Execution:Kubernetes/MaliciousFile 841
Execution:Container/MaliciousFile 842
Execution:EC2/SuspiciousFile 842
Execution:ECS/SuspiciousFile 843
Execution:Kubernetes/SuspiciousFile 844
Execution:Container/SuspiciousFile 844
Tipo de descoberta da Proteção contra malware para S3 845
Object:S3/MaliciousFile 845
Proteção contra malware para tipos de descoberta de Backup 846
Execution:EC2/MaliciousFile!Snapshot 846
Execution:EC2/MaliciousFile!AMI 847
Execution:EC2/MaliciousFile!RecoveryPoint 847
Execution:S3/MaliciousFile!RecoveryPoint 848
Tipos de descoberta da Proteção do RDS 848
CredentialAccess:RDS/AnomalousBehavior.SuccessfulLogin 849
CredentialAccess:RDS/AnomalousBehavior.FailedLogin 850
CredentialAccess:RDS/AnomalousBehavior.SuccessfulBruteForce 851
CredentialAccess:RDS/MaliciousIPCaller.SuccessfulLogin 852
CredentialAccess:RDS/MaliciousIPCaller.FailedLogin 853
Discovery:RDS/MaliciousIPCaller 853
CredentialAccess:RDS/TorIPCaller.SuccessfulLogin 854
CredentialAccess:RDS/TorIPCaller.FailedLogin 855
Discovery:RDS/TorIPCaller 855
Exfiltration:RDS/AnomalousBehavior 856
Impact:RDS/AnomalousBehavior.Drop 857
Impact:RDS/AnomalousBehavior.Delete 859
Exfiltration:RDS/MaliciousIPCaller 860
Exfiltration:RDS/TorIPCaller 861
Impact:RDS/MaliciousIPCaller 861
Impact:RDS/TorIPCaller 862
Tipos de descoberta da Proteção do Lambda 863
Backdoor:Lambda/C&CActivity.B 863
CryptoCurrency:Lambda/BitcoinTool.B 864

Trojan:Lambda/BlackholeTraffic 865
Trojan:Lambda/DropPoint 865
UnauthorizedAccess:Lambda/MaliciousIPCaller.Custom 866
UnauthorizedAccess:Lambda/TorClient 866
UnauthorizedAccess:Lambda/TorRelay 867
Tipos de descoberta de proteção de IA 867
Impact:IAMUser/AnomalousModelInvocation 868
Impact:IAMUser/CostHarvesting 870
Impact:IAMUser/PromptInjection.Direct 871
Tipos de descoberta desabilitados 873
PrivilegeEscalation:Kubernetes/PrivilegedContainer 875
Persistence:Kubernetes/ContainerWithSensitiveMount 875
Exfiltration:S3/ObjectRead.Unusual 876
Impact:S3/PermissionsModification.Unusual 877
Impact:S3/ObjectDelete.Unusual 877
Discovery:S3/BucketEnumeration.Unusual 878
Persistence:IAMUser/NetworkPermissions 879
Persistence:IAMUser/ResourcePermissions 879
Persistence:IAMUser/UserPermissions 880
PrivilegeEscalation:IAMUser/AdministrativePermissions 881
Recon:IAMUser/NetworkPermissions 882
Recon:IAMUser/ResourcePermissions 883
Recon:IAMUser/UserPermissions 883
ResourceConsumption:IAMUser/ComputeResources 884
Stealth:IAMUser/LoggingConfigurationModified 885
UnauthorizedAccess:IAMUser/ConsoleLogin 886
UnauthorizedAccess:EC2/TorIPCaller 886
Backdoor:EC2/XORDDOS 887
Behavior:IAMUser/InstanceLaunchUnusual 887
CryptoCurrency:EC2/BitcoinTool.A 888
UnauthorizedAccess:IAMUser/UnusualASNCaller 888
GuardDuty encontrando tipos por meio de recursos potencialmente afetados 889
GuardDuty tipos de descoberta ativa 889
Noções básicas e geração de descobertas 916
GuardDuty formato de busca 917
OBJETIVO DA AMEAÇA 918

GuardDuty mecanismo de verificação de detecção de malware 921
Amostras de descobertas 922
Geração de amostras de descobertas por meio do GuardDuty console ou da API 923
GuardDuty Resultados do teste 924
Considerações 925
GuardDuty descobertas que o script do testador pode gerar 926
Etapa 1: pré-requisitos 928
Etapa 2 - Implantar AWS recursos 929
Etapa 3 - Executar scripts do testador 931
Etapa 4 - Limpar os recursos AWS de teste 933
Solução de problemas comuns do 934
Página de descobertas no GuardDuty console 935
Navegar na página de descobertas 937
Níveis de gravidade das descobertas 938
Gravidade crítica 939
Gravidade alta 939
Gravidade média 939
Gravidade baixa 940
Detalhes da descoberta 940
Visão geral da descoberta 941
Recurso 942
Detalhes da descoberta da sequência de ataques 949
Regras de detecção personalizadas encontrando detalhes 957
Detalhes do usuário do banco de dados (DB) do RDS 959
Detalhes da descoberta do monitoramento de runtime 959
Detalhes de verificação de volumes do EBS 962
Detalhes de descobertas sobre a Proteção contra malware para EC2 963
Detalhes de descobertas sobre a Proteção contra malware para S3 964
Ação 965
Agente ou destino 967
Detalhes de geolocalização 968
Mais informações 968
Evidência 968
Comportamento anômalo 969
GuardDuty encontrando agregação 975
Gerenciando GuardDuty descobertas 976

GuardDuty Painel de resumo 977
Visão geral do 978
Conclusões 979
Tipos de descoberta mais comuns 980
Descobertas por gravidade 980
Contas com a maioria das descobertas 981
Recursos com descobertas 981
Descobertas que menos ocorrem 982
Cobertura de planos de proteção 982
Filtrando descobertas GuardDuty 983
Criando e salvando o conjunto de filtros no GuardDuty console 984
Criação e salvamento do conjunto de filtros usando GuardDuty API e CLI 986
Metadados do ciclo de vida 988
Filtros de propriedades em GuardDuty 989
Regras de supressão 1022
Usando regras de supressão com a Detecção de Ameaças Avançada 1023
Casos de uso comuns para regras de supressão e exemplos 1024
Criar regras de supressão 1027
Atualizando as regras de supressão 1032
Excluir regras de supressão 1035
Métricas da regra de supressão 1036
Listas de entidades e listas de endereços IP 1037
Noções básicas sobre listas de entidades e listas de endereços IP 1038
Considerações importantes sobre listas GuardDuty 1039
Formatos das listas 1040
Noções básicas sobre os status de listas 1049
Configuração de pré-requisitos para listas de entidades e listas de endereços IP 1050
Como adicionar e ativar uma lista de entidades ou lista de IPs 1052
Atualizando uma lista de entidades ou lista de endereços IP 1058
De-activating lista de entidades ou lista de endereços IP 1063
Excluindo lista de entidades ou lista de endereços IP 1066
Exportar as descobertas geradas para bucket do Amazon S3 1069
Considerações 1069
Etapa 1: Permissões necessárias para configurar a exportação de descobertas 1071
Etapa 2: Anexar política à sua chave do KMS 1071
Etapa 3: Anexar uma política ao bucket Amazon S3 1073

Etapa 4: Exportar descobertas para um bucket do S3 (console) 1077
Etapa 5 — Frequência de exportação de descobertas 1078
Processando descobertas com EventBridge 1079
EventBridge frequência de notificação em GuardDuty 1080
Configurar um tópico e um endpoint do Amazon SNS 1081
Usando EventBridge com GuardDuty 1082
Criar uma regra de EventBridge 1084
EventBridge regra para ambientes com várias contas 1091
Entendendo CloudWatch os registros e os motivos para ignorar recursos 1092
CloudWatch Registros de auditoria na proteção contra GuardDuty malware para EC2 1093
GuardDuty Proteção contra malware para retenção de registros do EC2 1095
Razões para ignorar o recurso 1095
Denunciando resultado falso positivo na verificação de malware para EC2 1100
Relatando resultado falso positivo de verificação de objetos S3 1101
Relatando um resultado falso positivo do escaneamento de malware do Backup 1102
Correção de descobertas 1104
Como corrigir uma instância do Amazon EC2 potencialmente comprometida 1104
Como corrigir um bucket do S3 possivelmente comprometido 1106
Recomendações com base em necessidades específicas de acesso a buckets do S3 1108
Como corrigir um objeto do S3 possivelmente malicioso 1109
Corrigindo um snapshot do EBS potencialmente comprometido 1109
Corrigindo uma AMI do EC2 potencialmente comprometida 1110
Corrigindo um ponto de recuperação EC2 potencialmente comprometido 1111
Corrigindo um ponto de recuperação S3 potencialmente comprometido 1112
Como corrigir um cluster do ECS possivelmente comprometido 1113
Correção de problemas potencialmente comprometidos AWS credenciais 1114
Como corrigir um contêiner autônomo possivelmente comprometido 1116
Como corrigir as descobertas da Proteção do EKS 1117
Possíveis problemas de configuração 1118
Como corrigir usuários do Kubernetes possivelmente comprometidos 1118
Como corrigir pods do Kubernetes possivelmente comprometidos 1121
Como corrigir imagens de contêiner possivelmente comprometidas 1123
Como corrigir pods do Kubernetes potencialmente comprometidos 1124
Como corrigir as descobertas do Monitoramento de runtime 1124
Como corrigir imagens de contêiner comprometidas 1126
Corrigir um banco de dados possivelmente comprometido 1127

Corrigir um banco de dados potencialmente comprometido com eventos de login bem-sucedidos 1127
Corrigindo um banco de dados potencialmente comprometido com eventos de login falhados 1128
Corrigindo um banco de dados potencialmente comprometido com atividade de exfiltração anômala 1130
Corrigindo um banco de dados potencialmente comprometido com atividade destrutiva anômala 1131
Corrigir remediar credenciais potencialmente comprometidas 1133
Restringir o acesso à rede 1133
Correção de uma função do Lambda comprometida 1134
Monitorando o uso e estimando custos 1135
Métricas CloudWatch de uso da Amazon 1135
Detalhes métricos 1135
Proteção contra malware para S3 1138
Entendendo GuardDuty o uso 1140
GuardDuty Processamento de eventos 1140
GuardDuty Cobranças de processamento do VPC Flow Logs para instâncias monitoradas pelo GuardDuty Runtime Monitoring 1140
Estimando GuardDuty o custo 1140
Utilizar AWS Calculadora de preços 1141
Clientes do Security Hub 1142
Nomes de recursos para planos de proteção na API 1143
Mudar de fontes de dados para atributos 1143
GuardDuty Mudanças na API 1143
Comparação de atributos com fontes de dados 1144
Como funcionam as APIs com atributos 1145
Como incorporar alterações de atributos nas APIs 1145
Recurso mapeado GuardDuty 1146
Segurança 1149
Proteção de dados 1150
Criptografia em repouso 1151
Criptografia em trânsito 1151
Optar por não usar seus dados para melhorar o serviço 1151
Fazendo login com CloudTrail 1153
GuardDuty informações em CloudTrail 1153

GuardDuty eventos do plano de controle em CloudTrail 1154
GuardDuty eventos de dados em CloudTrail 1154
Exemplo: entradas do arquivo de GuardDuty log 1156
Gerenciamento de Identidade e Acesso 1158
Público 1159
Autenticação com identidades 1159
Gerenciar o acesso usando políticas 1161
Como a Amazon GuardDuty trabalha com o IAM 1162
Identity-based exemplos de políticas 1168
Uso de perfis vinculados ao serviço 1178
AWS políticas gerenciadas 1188
Solução de problemas 1206
Validação de conformidade 1208
Resiliência 1209
Segurança da infraestrutura 1209
Endpoints da VPC (AWS PrivateLink) 1210
Considerações sobre GuardDuty VPC endpoints 1210
Criação de uma interface VPC endpoint para GuardDuty 1210
Criação de uma política de VPC endpoint para GuardDuty 1211
Sub-redes compartilhadas 1211
Integração com serviços AWS de segurança 1212
Integrando com GuardDuty AWS Security Hub CSPM 1212
Integração GuardDuty com o Amazon Detective 1212
AWS Security Hub CSPM integração 1212
Como a Amazon GuardDuty envia descobertas para AWS Security Hub CSPM 1213
Visualizando GuardDuty descobertas em AWS Security Hub CSPM 1214
Habilitar e configurar a integração 1235
Usando GuardDuty controles no Security Hub CSPM 1235
Interrupção da publicação de descobertas no CSPM do Security Hub 1235
Integração do Amazon Detective 1235
Habilitar a integração 1236
Passando para o Amazon Detective a partir de uma descoberta GuardDuty 1236
Usando a integração com um ambiente de GuardDuty várias contas 1237
Suspender ou desabilitar 1238
GuardDuty anúncios 1240
Formato da mensagem do Amazon SNS 1246

GuardDuty cotas 1251
Support para instâncias gerenciadas 1258
Solução de problemas 1259
Exportar as descobertas para o Amazon S3 - erro de acesso 1259
Proteção contra malware para problemas EC2 1260
Falta (obrigatório) AWS Organizations permissão de gerenciamento ao ativar a verificação de GuardDuty-initiated malware 1260
Estou iniciando uma verificação de On-demand malware, mas isso resulta na falta de um erro de permissões necessárias. 1260
Eu recebo um GetRole erro `iam:` ao trabalhar com o Malware Protection for EC2. 1261
Sou uma conta de GuardDuty administrador que precisa ativar a verificação de GuardDuty-initiated malware, mas não usa AWS política gerenciada: AmazonGuardDutyFullAccess para gerenciar GuardDuty. 1261
Problemas de Runtime Monitoring 1261
Problemas de cobertura de runtime 1261
Solução de problemas de falta de memória 1262
Meu AWS Step Functions o fluxo de trabalho está falhando inesperadamente 1262
Outros problemas de solução de problemas 1263
Regiões e endpoints 1264
Region-specific disponibilidade de recursos 1264
Ações e parâmetros legados 1267
Histórico do documento 1269
Atualizações anteriores 1380
..... mccclxxxi

O que é a Amazon GuardDuty?

GuardDuty A Amazon é um serviço de detecção de ameaças que monitora, analisa e processa continuamente fontes de AWS dados e registros em seu AWS ambiente. GuardDuty usa feeds de inteligência de ameaças, como listas de endereços IP e domínios maliciosos, hashes de arquivos e modelos de aprendizado de máquina (ML) para identificar atividades suspeitas e potencialmente maliciosas em seu ambiente. AWS A lista a seguir fornece uma visão geral dos possíveis cenários de ameaças que GuardDuty podem ajudá-lo a detectar:

- Credenciais comprometidas e extraídas. AWS
- Extração e destruição de dados que podem levar a um evento de ransomware. Padrões incomuns de eventos de login nas versões de mecanismo compatíveis com os bancos de dados Amazon Aurora e Amazon RDS que indicam comportamento anômalo.
- Atividade de criptomineração não autorizada em suas instâncias do Amazon Elastic Compute Cloud (Amazon EC2) e em workloads de contêineres.
- Presença de malware em suas instâncias do Amazon EC2 e em workloads de contêineres e arquivos recém-carregados em buckets do Amazon Simple Storage Service (Amazon S3).
- Eventos no nível do sistema operacional, na rede e em arquivos que indicam comportamento não autorizado em clusters do Amazon Elastic Kubernetes Service (Amazon EKS), Amazon Elastic Container Service (Amazon ECS) - tarefas AWS Fargate e em instâncias do Amazon EC2 e workloads de contêineres.

O vídeo a seguir fornece uma visão geral de como GuardDuty ajuda você a detectar ameaças em seu AWS ambiente.

O que é a Amazon GuardDuty

Conteúdo

- Características do GuardDuty
- Compatibilidade com PCI DSS
- Preços em GuardDuty
- Acessando GuardDuty

Características do GuardDuty

Aqui estão algumas das principais maneiras pelas quais a Amazon GuardDuty pode ajudar você a monitorar, detectar e gerenciar possíveis ameaças em seu AWS ambiente.

Monitora continuamente fontes de dados e registros de eventos específicos

- Detecção básica de ameaças — Quando você ativa GuardDuty uma Conta da AWS, começa GuardDuty automaticamente a ingerir as fontes de dados fundamentais associadas a essa conta. Essas fontes de dados incluem eventos AWS CloudTrail de gerenciamento, registros de fluxo da VPC (de instâncias do Amazon EC2) e registros de DNS. Você não precisa habilitar

mais nada para começar GuardDuty a analisar e processar essas fontes de dados para gerar descobertas de segurança associadas. Para obter mais informações, consulte GuardDuty fontes de dados fundamentais.

- Detecção estendida de ameaças — Esse recurso detecta ataques em vários estágios que abrangem fontes de dados fundamentais, vários tipos de AWS recursos e tempo, dentro de um. Conta da AWS Pode haver vários eventos na sua conta que, individualmente, não se apresentam como uma ameaça clara. No entanto, quando esses eventos são observados em uma sequência indicativa de uma atividade suspeita, GuardDuty identifica-a como uma sequência de ataque. GuardDuty notifica você gerando o tipo de descoberta da sequência de ataque associada para fornecer detalhes sobre a sequência de ataque observada.

  Sem nenhum custo adicional associado, a Detecção Estendida de Ameaças é ativada automaticamente para cada um Conta da AWS quando eles são ativados GuardDuty. Esse recurso não exige que você habilite nenhum plano de proteção focado no caso de uso. No entanto, para aumentar a amplitude da segurança de seus recursos do Amazon S3 GuardDuty , recomenda habilitar a Proteção do S3 em sua conta. Isso ajudará a Detecção de Ameaças Avançada a identificar ataques em vários estágios que potencialmente afetam seus recursos do Amazon S3.

  Para obter mais informações sobre como esse recurso funciona e quais cenários de ameaça ele abrange, consulte GuardDuty Detecção estendida de ameaças.

- Investigação (prévia) — A GuardDuty investigação fornece uma análise de AI-powered segurança de suas GuardDuty descobertas. Você pode criar investigações para analisar descobertas específicas, contas ou toda a sua organização e receber resumos estruturados de investigações com avaliação de risco, pontuação de confiança, classificação MITRE ATT&CK® e próximas etapas acionáveis. Para obter mais informações, consulte GuardDuty Investigação (Pré-visualização).

- Regras de detecção personalizadas — As regras de detecção personalizadas são uma biblioteca organizada de regras de detecção na Amazon GuardDuty que estão alinhadas às técnicas dos agentes de ameaças. Cada regra detecta uma técnica específica avaliando campos em eventos de AWS CloudTrail gerenciamento ou em eventos de Runtime Monitoring do agente de GuardDuty segurança. Você pode navegar, ativar e gerenciar regras no GuardDuty console ou por meio da GuardDuty API. Para obter mais informações, consulte Regras de detecção personalizadas em GuardDuty.

- Use-case planos de GuardDuty proteção focados — Para maior visibilidade da detecção de ameaças na segurança do seu AWS ambiente, GuardDuty oferece planos de proteção

dedicados que você pode optar por ativar. Os planos de proteção ajudam você a monitorar registros e eventos de outros AWS serviços. Essas fontes incluem registros de auditoria do EKS, atividade de login do RDS, eventos de dados do Amazon S3 CloudTrail em, volumes do EBS, monitoramento de tempo de execução no Amazon EKS, Amazon EC2 e Amazon ECS-Fargate, registros de atividades de rede Lambda e AWS CloudTrail eventos de dados do Amazon Bedrock, Amazon AgentCore Bedrock e Amazon AI for AI for AI Protection. SageMaker GuardDutyconsolida essas fontes de log e eventos sob o termo - Características. Você pode habilitar um ou mais planos de proteção dedicados em um suporte Região da AWS a qualquer momento. GuardDuty iniciará o monitoramento, o processamento e a análise das atividades com base no plano de proteção ativado. Para obter mais informações sobre cada plano de proteção e como ele funciona, consulte o documento do plano de proteção correspondente.

Quando você ativa GuardDuty pela primeira vez, ativa GuardDuty automaticamente todos os planos de proteção, exceto o Runtime Monitoring, para sua conta, e os inclui no teste gratuito de 30 dias. Você pode desativar qualquer plano de proteção a qualquer momento. Se você já é um GuardDuty cliente, um plano de proteção que é iniciado após a ativação não GuardDuty é ativado automaticamente, e você pode optar por ativá-lo. Para obter informações sobre quais planos de proteção estão habilitados por padrão, consulteUsando o GuardDuty teste gratuito de 30 dias.

Plano de proteção	Description
Proteção da IA	Detecta ameaças às suas cargas de trabalho de IA que usam o Amazon Bedrock, o Amazon Bedrock AgentCore e o Amazon SageMaker AI, como invocações de modelos anômalos e ataques de coleta de custos.
Proteção do S3	Identifica possíveis riscos de segurança, como tentativas de exfiltração e destruição de dados em seus buckets do Amazon S3.
Proteção do EKS	Monitoramento de logs de auditoria do EKS analisa os logs dos clusters do Amazon EKS em busca de atividades potencialmente mal-intencionadas e suspeitas.

Plano de proteção	Description
Monitoramento de runtime	Monitora e analisa eventos em nível de sistema operacional em seu Amazon EKS, Amazon EC2 e Amazon ECS (inclusive AWS Fargate), para detectar possíveis ameaças em runtime.
Proteção contra malware para o EC2	Detecta a possível presença de malware ao escanear os volumes do Amazon EBS associados às suas instâncias do Amazon EC2. Há uma opção para usar esse recurso sob demanda.
Proteção contra malware para S3	Detecta a presença potencial de malware nos objetos recém-carregados em seus buckets do Amazon S3. Há uma opção para usar esse recurso sob demanda.
Proteção contra malware para AWS backup	Detecta a presença potencial de malware examinando recursos de backup, incluindo instantâneos do EBS, AMIs do EC2 e pontos de recuperação de backup AWS . Há uma opção para usar esse recurso sob demanda.
Proteção do RDS	Analisa e traça o perfil de atividade de login RDS em busca de possíveis ameaças de acesso aos seus bancos de dados do Amazon Aurora e Amazon RDS.
Proteção do Lambda	Monitora os registros de atividades da rede Lambda, começando com os registros de fluxo da VPC, para detectar ameaças às suas funções. AWS Lambda Exemplos dessas ameaças em potencial incluem criptomineração e comunicação com servidores maliciosos.

A proteção contra malware para S3 é um recurso independente

GuardDuty oferece flexibilidade para usar o Malware Protection for S3 de forma independente, sem habilitar o GuardDuty serviço Amazon. Para obter mais informações sobre os conceitos básicos de Proteção de Malware para S3, consulteGuardDuty

Proteção contra malware para S3. Para usar todos os outros planos de proteção, você deve ativar o GuardDuty serviço.

Gerencie o ambiente de várias contas

Você pode gerenciar um AWS ambiente de várias contas usando o método de convite AWS Organizations (recomendado) ou antigo. Para obter mais informações, consulte Gerenciar várias contas.

Gera descobertas de segurança para ameaças detectadas

Quando GuardDuty detecta possíveis ameaças à segurança associadas aos seus AWS recursos, ele começa a gerar descobertas de segurança que fornecem informações sobre o recurso potencialmente comprometido. Depois de habilitar GuardDuty em sua conta, gere Amostras de descobertas para ver o associadoDetalhes da descoberta. Para obter uma lista completa de descobertas de segurança, consulteGuardDuty tipos de descoberta.

Com GuardDuty, você também pode usar um script de testador que gera descobertas GuardDuty de segurança específicas para entender como analisar e responder às GuardDuty descobertas. Para obter mais informações, consulte GuardDuty Resultados do teste em contas dedicadas.

Avaliando e gerenciando descobertas de segurança

GuardDuty consolida suas descobertas de segurança em todas as contas e exibe os resultados no painel de resumo no GuardDuty console. Você também pode recuperar descobertas por meio da AWS Security Hub CSPM API ou do AWS SDK. AWS Command Line Interface Com uma visão ampla do seu status de segurança atual, você pode identificar tendências e potenciais problemas e tomar as medidas de correção necessárias. Para obter mais informações, consulte Gerenciando GuardDuty descobertas.

Integre com serviços AWS de segurança relacionados

Para ajudá-lo ainda mais a analisar e investigar as tendências de segurança em seu AWS ambiente, considere usar os seguintes serviços AWS relacionados à segurança em combinação com o. GuardDuty

- AWS Security Hub CSPM— Esse serviço oferece uma visão abrangente do estado de segurança de seus AWS recursos e ajuda a verificar seu AWS ambiente em relação aos padrões e às melhores práticas de segurança do setor. Ele faz isso parcialmente consumindo, agregando, organizando e priorizando suas descobertas de segurança de vários AWS serviços (incluindo Amazon Macie) e produtos compatíveis da AWS Partner Network (APN). O Security

Hub CSPM ajuda você a analisar suas tendências de segurança e identificar os problemas de segurança de maior prioridade em seu AWS ambiente.

Para obter informações sobre como usar o GuardDuty CSPM do Security Hub em conjunto, consulte. Integrando com GuardDuty AWS Security Hub CSPM Para saber mais sobre o CSPM do Security Hub, consulte o Guia do AWS Security Hub Usuário.

- O Amazon Detective - Este serviço ajuda a analisar, investigar e identificar rapidamente a causa raiz de descobertas de segurança ou atividades suspeitas. Detective coleta automaticamente os dados de registro de seus recursos. AWS Em seguida, ele usa machine learning, análises estatísticas e a teoria de grafos para gerar visualizações que ajudam a realizar investigações de segurança eficazes com maior rapidez. O Detective faz a pré-construção de agregações de dados, resumos e contexto predefinidos que podem ajudar você a analisar e determinar a natureza e a extensão de possíveis problemas de segurança.

  Para obter informações sobre como usar o GuardDuty Detective em conjunto, consulte. Integração GuardDuty com o Amazon Detective Para saber mais sobre Detective, consulte o Guia do usuário do Amazon Detective.
- Amazon EventBridge — Esse serviço ajuda você a receber notificações e responder às descobertas GuardDuty de segurança quase em tempo real. GuardDuty cria um evento quando há uma mudança nas descobertas. Você pode escolher com que frequência deseja receber as notificações EventBridge. Para obter mais informações, consulte O que é a Amazon EventBridge no Guia EventBridge do usuário da Amazon.

Compatibilidade com PCI DSS

GuardDuty suporta o processamento, armazenamento e transmissão de dados de cartão de crédito por um comerciante ou provedor de serviços e foi validado como compatível com o Padrão de Segurança de Dados (DSS) do Setor de Cartões de Pagamento (PCI). Para obter mais informações sobre o PCI DSS, incluindo como solicitar uma cópia do PCI AWS Compliance Package, consulte PCI DSS Nível 1.

Para obter mais informações, consulte Novo teste de terceiros que compara GuardDuty a Amazon com sistemas de detecção de intrusões de rede no AWS blog de segurança.

Preços em GuardDuty

Esta seção se concentra no Nível gratuito da AWS modelo GuardDuty usado em vários planos de proteção e em como você pode visualizar os custos de uso estimados e reais. Se você estiver procurando os detalhes de preços associados a todos os planos de proteção nas regiões suportadas, consulte os GuardDutypreços.

Nível gratuito da AWS

Nível gratuito da AWS ajuda você a explorar e experimentar Serviços da AWS gratuitamente até os limites especificados para cada serviço. Há três categorias - 12 meses gratuitos, sempre gratuitos e testes gratuitos de curto prazo. A Amazon GuardDuty pertence à categoria de teste gratuito de curto prazo e oferece um teste gratuito de 30 dias. Ao continuar usando GuardDuty após o término do teste gratuito, você começa a incorrer em custos com base em como usa esse serviço.

[1] exceção ao GuardDuty teste gratuito de 30 dias

On-demand a verificação de malware (em Proteção contra malware para EC2) e a Proteção contra malware para S3 não se enquadram na categoria de teste gratuito de curto prazo de GuardDuty 30 dias. A proteção contra malware para S3 inclui um nível gratuito, enquanto a verificação de On-demand malware segue um modelo de custo de pagamento conforme o uso. Não há um teste gratuito de 30 dias ou um modelo de custo de nível gratuito com verificação de On-demand malware.

Usando o GuardDuty teste gratuito de 30 dias

Ao usar GuardDuty pela primeira vez em um Região da AWS, você Conta da AWS é automaticamente inscrito em um teste gratuito de 30 dias nessa região. Alguns dos planos de proteção também serão habilitados automaticamente e incluídos no teste gratuito de 30 dias. Como GuardDuty é um serviço regional, quando você o ativa pela primeira vez em uma região diferente, sua conta receberá um teste gratuito de 30 dias dessa GuardDuty região. Ao trabalhar com várias contas em uma GuardDuty organização, cada conta tem seu próprio teste gratuito de 30 dias.

Use a tabela a seguir para verificar quais planos de proteção estão habilitados por GuardDuty padrão e sua disponibilidade de teste gratuito.

Plano de proteção	Ativado por padrão com GuardDuty	Disponibilidade de teste gratuito separado[2]
Proteção do EKS	Sim	Sim
Proteção do S3	Sim	Sim
Monitoramento de runtime	Não	Sim
Proteção contra malware para o EC2 – GuardDuty-initiated escaneamento de malware	Sim	Sim
Proteção contra malware para o EC2 – On-demand escaneamento de malware em GuardDuty	Não	Não [1]
GuardDuty Proteção contra malware para S3	Não	Não [1]
Proteção do RDS	Sim	Sim
Proteção do Lambda	Sim	Sim
Proteção contra malware para AWS backup	Não	Não

[2] Quando você ativa GuardDuty pela primeira vez, os planos de proteção (exceto o Runtime Monitoring) são automaticamente ativados e incluídos no teste gratuito inicial de 30 dias. Quando uma GuardDuty conta existente ativa um novo plano de proteção após o término do teste GuardDuty gratuito inicial, esse plano de proteção vem com seu próprio teste gratuito de 30 dias. Para obter informações sobre o teste gratuito associado a cada plano de proteção.

Veja o custo estimado de uso durante o teste gratuito — Durante o teste gratuito de 30 dias GuardDuty e, potencialmente, um plano de proteção, GuardDuty fornece o custo estimado de uso da sua conta. Se você for uma conta de GuardDuty administrador delegado, poderá ver o custo total de uso estimado e o detalhamento em nível de conta de todas as contas de membros que foram ativadas. GuardDuty Para obter mais informações, consulte Monitorando GuardDuty o uso e estimando custos.

Custo de uso após o término do teste gratuito — Ao continuar usando GuardDuty ou qualquer um de seus planos de proteção após o término do teste gratuito, você começará a incorrer nos custos de uso associados. Para ver sua fatura, navegue até Cost Explorer no https://console.aws.amazon.com/costmanagement/console. Para obter mais informações sobre o faturamento da AWS conta, consulte o Guia AWS Billing do usuário.

Usando a proteção contra malware para S3 com nível gratuito

A proteção contra malware para S3 inclui um nível gratuito associado ao seu Contas da AWS. Para obter mais informações, consulte Preço e custo de uso da Proteção contra Malware para S3.

Acessando GuardDuty

A Amazon GuardDuty está disponível na maioria Regiões da AWS. Para obter uma lista das regiões em GuardDuty que está disponível atualmente, consulteRegiões e endpoints.

Você pode usar GuardDuty de qualquer uma das seguintes formas:

GuardDuty console

https://console.aws.amazon.com/guardduty/

O console é uma interface baseada em navegador para acesso e uso do GuardDuty. O GuardDuty console fornece acesso à sua GuardDuty conta, dados e recursos.

AWS Command Line Interface

Com AWS Command Line Interface (AWS CLI), você pode emitir comandos na linha de comando do seu sistema para realizar GuardDuty tarefas e AWS tarefas. Os AWS CLI comandos são úteis se você quiser criar scripts que executem tarefas.

Para obter informações sobre instalação e uso AWS CLI, consulte o Guia AWS Command Line Interface do usuário. Para ver os AWS CLI comandos disponíveis para GuardDuty, consulte Referência de AWS CLI comandos.

GuardDuty API HTTPS

Você pode acessar GuardDuty e AWS programaticamente usando a API GuardDuty HTTPS, que permite emitir solicitações HTTPS diretamente para o serviço. Para obter mais informações, consulte a Amazon GuardDuty API Reference.

AWS SDKs

AWS fornece kits de desenvolvimento de software (SDKs) que consistem em bibliotecas e exemplos de código para várias linguagens e plataformas de programação (Java, Python, Ruby, .NET, iOS, Android e muito mais). Os SDKs são uma forma conveniente de criar acesso programático ao GuardDuty. Para obter informações sobre os SDKs AWS , incluindo como fazer download e instalá-los, consulte Ferramentas da Amazon Web Services.

Conceitos e termos-chave na Amazon GuardDuty

Ao começar a usar a Amazon GuardDuty, você pode se beneficiar ao aprender sobre seus conceitos e os principais termos associados.

Conta

Uma conta padrão da Amazon Web Services (AWS) que contém seus AWS recursos. Você pode fazer login AWS com sua conta e ativar GuardDuty.

Você também pode convidar outras contas para ativar GuardDuty e se associar à sua AWS conta em GuardDuty. Se seus convites forem aceitos, sua conta será designada como conta GuardDuty de administrador e as contas adicionadas se tornarão suas contas de membros. Em seguida, você pode visualizar e gerenciar as GuardDuty descobertas dessas contas em nome delas.

Os usuários da conta de administrador podem configurar GuardDuty , visualizar e gerenciar GuardDuty as descobertas de sua própria conta e de todas as contas de membros. Para obter informações sobre o número de contas de membros que sua conta de administrador pode gerenciar, consulte GuardDuty cotas.

Os usuários das contas dos membros podem configurar GuardDuty , visualizar e gerenciar GuardDuty as descobertas em suas contas (por meio do console GuardDuty de gerenciamento ou GuardDuty da API). Os usuários de contas de membro não podem visualizar ou gerenciar descobertas nas contas de outros membros.

E não Conta da AWS pode ser uma conta de GuardDuty administrador e uma conta de membro ao mesmo tempo. Uma conta da Conta da AWS pode aceitar apenas um convite de associação. Aceitar um convite de associação é opcional.

Para obter mais informações, consulte Gerenciando várias contas na Amazon GuardDuty.

Sequência de ataques

Uma sequência de ataque é uma correlação de vários eventos que, conforme observado por GuardDuty, aconteceram em uma sequência específica que corresponde ao padrão de uma atividade suspeita. GuardDuty usa sua Detecção de Ameaças Avançada capacidade de detectar esses ataques em vários estágios que abrangem fontes de dados, AWS recursos e cronograma fundamentais em sua conta.

A lista a seguir explica resumidamente os principais termos associados às sequências de ataque:

- Indicadores – fornece informações sobre o motivo pelo qual uma sequência de eventos se alinha com uma possível atividade suspeita.
- Sinais — Um sinal é uma atividade de API GuardDuty observada ou uma GuardDuty descoberta já detectada em sua conta. Ao correlacionar os eventos que foram observados em uma sequência específica em sua conta, GuardDuty identifica uma sequência de ataque.

  Há eventos em sua conta que não são indicativos de uma possível ameaça. GuardDuty os considera sinais fracos. No entanto, quando sinais e GuardDuty descobertas fracos são observados em uma sequência específica que, quando correlacionada, se alinha a uma atividade potencialmente suspeita, GuardDuty gera uma descoberta da sequência de ataque.
- Endpoints – informações sobre endpoints de rede que um agente de ameaça potencialmente usou em uma sequência de ataque.

Detector

A Amazon GuardDuty é um serviço regional. Quando você ativa GuardDuty um determinado Região da AWS, você Conta da AWS é associado a um ID de detector. Esse ID alfanumérico de 32 caracteres é exclusivo para sua conta nessa região. Por exemplo, quando você ativa GuardDuty a mesma conta em uma região diferente, sua conta é associada a uma ID de detector diferente. O formato de um detectorId é `12abc34d567e8fa901bc2d34e56789f0`.

Todas as GuardDuty descobertas, contas e ações sobre o gerenciamento de descobertas e o GuardDuty serviço usam o ID do detector para executar uma operação de API.

Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no https://console.aws.amazon.com/guardduty/console ou execute a ListDetectorsAPI.

> **Note**
>
> Em ambientes de várias contas, todas as descobertas de contas-membro são acumuladas no detector da conta de administrador.

Algumas GuardDuty funcionalidades são configuradas por meio do detector, como a configuração da frequência de notificação de CloudWatch eventos e a ativação ou desativação de planos de proteção opcionais GuardDuty para processamento.

Usando a proteção contra malware para S3 em GuardDuty

Quando você ativa a Proteção contra Malware para S3 em uma conta em que GuardDuty está ativada, as ações da Proteção contra Malware para S3, como ativar, editar e desativar um recurso protegido, não são associadas à ID do detector.

Quando você não ativa GuardDuty e escolhe a opção de detecção de ameaças Malware Protection for S3, não há um ID de detector criado para sua conta.

Fontes de dados fundamentais

A origem ou a localização de um conjunto de dados. Para detectar uma atividade não autorizada ou inesperada em seu AWS ambiente. GuardDuty analisa e processa dados de registros de AWS CloudTrail eventos, eventos de AWS CloudTrail gerenciamento, eventos de AWS CloudTrail dados para S3, registros de fluxo de VPC, registros de DNS, consulte. GuardDuty fontes de dados fundamentais

Recurso

Um objeto de recurso configurado para seu plano de GuardDuty proteção ajuda a detectar uma atividade não autorizada ou inesperada em seu AWS ambiente. Cada plano GuardDuty de proteção configura o objeto de recurso correspondente para analisar e processar dados. Alguns dos objetos de atributo incluem logs de auditoria do EKS, monitoramento de atividades de login do RDS, logs de atividade de rede Lambda e volumes do EBS. Para obter mais informações, consulte Nomes de recursos para planos de proteção na GuardDuty API.

Descoberta

Um possível problema de segurança descoberto pelo GuardDuty. Para obter mais informações, consulte Entendendo e gerando GuardDuty descobertas da Amazon.

As descobertas são exibidas no GuardDuty console e contêm uma descrição detalhada do problema de segurança. Você também pode recuperar suas descobertas geradas chamando as operações GetFindingse da ListFindingsAPI.

Você também pode ver suas GuardDuty descobertas por meio de CloudWatch eventos da Amazon. GuardDuty envia descobertas para a Amazon CloudWatch por meio do protocolo HTTPS. Para obter mais informações, consulte Processando GuardDuty descobertas com a Amazon EventBridge.

Perfil do IAM

Essa é a função do IAM com as permissões necessárias para verificar o objeto do S3. Quando a marcação de objetos digitalizados está ativada, PassRole as permissões do IAM ajudam a GuardDuty adicionar tags ao objeto digitalizado.

Recurso do plano de Proteção contra malware

Depois de habilitar o Malware Protection for S3 para um bucket, GuardDuty cria um recurso do plano de Proteção contra Malware. Esse recurso está associado ao ID do plano de Proteção contra Malware, um identificador exclusivo para seu bucket protegido. Use o recurso do plano de Proteção contra malware para realizar operações de API em um recurso protegido.

Bucket protegido (recurso protegido)

Um bucket do Amazon S3 é considerado protegido quando você ativa a Proteção contra Malware para S3 para esse bucket e seu status de proteção muda para Ativo.

GuardDuty suporta somente um bucket S3 como recurso protegido.

Status de proteção

O status associado ao seu recurso do plano de Proteção contra malware. Depois de ativar a Proteção contra Malware para S3 em seu bucket, esse status representa se o bucket está ou não configurado corretamente.

Um prefixo de objeto S3

Em um bucket do Amazon Simple Storage Service (Amazon S3), use prefixos para organizar seu armazenamento. Um prefixo é um agrupamento lógico dos objetos em um bucket S3. Para obter mais informações, consulte Organizando e listando objetos no Guia de usuário do Amazon S3.

Opções de verificação

Quando a Proteção contra GuardDuty Malware para EC2 está ativada, ela permite que você especifique quais instâncias do Amazon EC2 e volumes do Amazon Elastic Block Store (EBS) devem ser verificados ou ignorados. Esse atributo permite que você adicione as tags existentes associadas às suas instâncias do EC2 e ao volume do EBS a uma lista de tags de inclusão ou de exclusão. Os recursos associados às tags que você adiciona a uma lista de tags de inclusão são verificados em busca de malware, e aqueles adicionados a uma lista de tags de exclusão não são examinados. Para obter mais informações, consulte Opções de verificação com tags definidas pelo usuário.

Retenção de snapshots

Quando a Proteção contra GuardDuty Malware para EC2 está ativada, ela oferece a opção de reter os instantâneos dos volumes do EBS em sua conta. AWS GuardDuty gera os volumes de réplica do EBS com base nos instantâneos dos seus volumes do EBS. Você pode reter os snapshots dos seus volumes do EBS somente se a verificação da Proteção contra malware para EC2 detectar malware nos volumes de réplica do EBS. Se nenhum malware for detectado nos volumes de réplica do EBS, GuardDuty excluirá automaticamente os instantâneos dos seus volumes do EBS, independentemente da configuração de retenção de instantâneos. Para obter mais informações, consulte Retenção de snapshots.

Regra de supressão

As regras de supressão permitem criar combinações muito específicas de atributos para suprimir descobertas. Por exemplo, você pode definir uma regra por meio do GuardDuty filtro para arquivar automaticamente `Recon:EC2/Portscan` somente dessas instâncias em uma VPC específica, executando uma AMI específica ou com uma tag EC2 específica. Essa regra resultaria em descobertas de varredura de portas sendo arquivadas automaticamente a partir das instâncias que atendem aos critérios. No entanto, ele ainda permite alertar se GuardDuty detectar essas instâncias conduzindo outras atividades maliciosas, como mineração de criptomoedas.

As regras de supressão definidas na conta do GuardDuty administrador se aplicam às contas dos GuardDuty membros. GuardDuty as contas dos membros não podem modificar as regras de supressão.

Com as regras de supressão, GuardDuty ainda gera todas as descobertas. As regras de supressão fornecem supressão de descobertas e mantêm um histórico completo e imutável de toda a atividade.

Normalmente, as regras de supressão são usadas para ocultar descobertas determinadas como falsos positivos para o ambiente e reduzir o ruído de descobertas de baixo valor para que você possa se concentrar em ameaças maiores. Para obter mais informações, consulte Regras de supressão em GuardDuty.

Lista de IPs confiáveis

Uma lista de endereços IP confiáveis para comunicação altamente segura com seu AWS ambiente. GuardDuty não gera descobertas com base em listas de IP confiáveis. Para obter mais informações, consulte Customizing threat detection with entity lists and IP address lists.

Lista de IPs de ameaças

Uma lista de endereços IP mal-intencionados conhecidos. Além de gerar descobertas devido a uma atividade potencialmente suspeita, GuardDuty também gera descobertas com base nessas listas de ameaças. Para obter mais informações, consulte Customizing threat detection with entity lists and IP address lists.

Começando com GuardDuty

Este tutorial fornece uma introdução prática ao. GuardDuty Os requisitos mínimos para habilitação GuardDuty como conta independente ou como GuardDuty administrador AWS Organizations são abordados na Etapa 1. As etapas 2 a 5 abrangem o uso de recursos adicionais recomendados por GuardDuty para aproveitar ao máximo suas descobertas.

Tópicos

- Antes de começar
- Etapa 1: habilitar a Amazon GuardDuty
- Etapa 2: gerar descobertas de amostra e explorar as operações básicas
- Etapa 3: Configurar a exportação de GuardDuty descobertas para um bucket do Amazon S3
- Etapa 4: configurar alertas de GuardDuty busca por meio do SNS
- Próximas etapas

Antes de começar

GuardDuty é um serviço de detecção de ameaças que monitora Fontes de dados fundamentais eventos de AWS CloudTrail gerenciamento, registros de fluxo da Amazon VPC e registros de consultas de Amazon Route 53 Resolver DNS. GuardDutytambém analisa os recursos associados a seus tipos de proteção somente se você os ativar separadamente. Os recursos incluem registros de auditoria do Kubernetes, atividade de login do RDS, eventos de AWS CloudTrail dados para Amazon S3, volumes do Amazon EBS, monitoramento de tempo de execução e registros de atividades da rede Lambda. O uso dessas fontes de dados e recursos (se ativado) GuardDuty gera descobertas de segurança para sua conta.

Depois de habilitar GuardDuty, ele começa a monitorar sua conta em busca de possíveis ameaças com base nas atividades nas fontes de dados fundamentais. Por padrão, Detecção de Ameaças Avançada está habilitado para todos os Contas da AWS que foram ativados GuardDuty. Esse recurso detecta sequências de ataques em vários estágios que abrangem várias fontes de dados, recursos (e tempo) da AWS na sua conta. Para detectar possíveis ameaças a AWS recursos específicos, você pode optar por ativar planos de proteção focados em casos de uso que GuardDuty ofereçam. Para obter mais informações, consulte Características do GuardDuty.

Não é necessário habilitar explicitamente nenhuma das fontes de dados fundamentais. Ao habilitar a Proteção do S3, não é necessário habilitar explicitamente o registro de eventos de dados do Amazon

S3. Da mesma forma, ao habilitar a proteção EKS, não é necessário habilitar explicitamente os logs de auditoria do Amazon EKS. A Amazon GuardDuty extrai fluxos independentes de dados diretamente desses serviços.

Para uma nova GuardDuty conta, alguns dos tipos de proteção disponíveis que são suportados em um Região da AWS são ativados e incluídos no período de teste gratuito de 30 dias por padrão. É possível desabilitar um ou todos eles. Se você já tem um plano GuardDuty habilitado, você pode optar por ativar qualquer um ou todos os planos de proteção que estão disponíveis em sua região. Conta da AWS Para obter uma descrição geral dos planos de proteção e de quais planos de proteção serão habilitados por padrão, consulte Preços em GuardDuty.

Ao ativar GuardDuty, considere os seguintes itens:

- GuardDuty é um serviço regional, o que significa que qualquer um dos procedimentos de configuração que você segue nesta página deve ser repetido em cada região com a qual você deseja monitorar GuardDuty.

  É altamente recomendável que você habilite GuardDuty em todas as AWS regiões suportadas. Isso permite GuardDuty gerar descobertas sobre atividades não autorizadas ou incomuns, mesmo em regiões que você não está usando ativamente. Isso também permite GuardDuty monitorar AWS CloudTrail eventos para AWS serviços globais, como o IAM. Se não GuardDuty estiver habilitado em todas as regiões suportadas, sua capacidade de detectar atividades que envolvam serviços globais será reduzida. Para obter uma lista completa das regiões onde GuardDuty está disponível, consulteRegiões e endpoints.
- Qualquer usuário com privilégios de administrador em uma AWS conta pode habilitar GuardDuty, no entanto, seguindo a melhor prática de segurança do menor privilégio, é recomendável criar uma função, usuário ou grupo do IAM para gerenciar GuardDuty especificamente. Para obter informações sobre as permissões necessárias para habilitar, GuardDuty consultePermissões necessárias para habilitar GuardDuty.
- Quando você ativa GuardDuty pela primeira vez em qualquer um Região da AWS, por padrão, ele também ativa todos os tipos de proteção disponíveis que são suportados nessa região, incluindo a Proteção contra Malware para EC2. GuardDuty cria uma função vinculada ao serviço para sua conta chamada. `AWSServiceRoleForAmazonGuardDuty` Essa função inclui as permissões e as políticas de confiança que GuardDuty permitem consumir e analisar eventos diretamente do GuardDuty fontes de dados fundamentais para gerar descobertas de segurança. A Proteção contra malware para o EC2 cria outra função vinculada ao serviço para sua conta chamada `AWSServiceRoleForAmazonGuardDutyMalwareProtection`. Essa função inclui as permissões e as políticas de confiança que permitem que o Malware Protection for EC2 realize

verificações sem agentes para detectar malware em sua conta. GuardDuty Ele permite GuardDuty criar um instantâneo do volume do EBS em sua conta e compartilhar esse instantâneo com a GuardDuty conta de serviço. Para obter mais informações, consulte Service-linked permissões de função para GuardDuty. Para obter mais informações sobre as funções vinculadas a um serviço, consulte Como usar funções vinculadas a serviços.

- Quando você ativa GuardDuty pela primeira vez em qualquer região, sua AWS conta é automaticamente inscrita em um teste GuardDuty gratuito de 30 dias para essa região.

O vídeo a seguir explica como uma conta de administrador pode começar a usá-la GuardDuty e ativá-la em várias contas de membros.

Introdução: Habilitando a Amazon GuardDuty para ambientes autônomos ou com várias contas

Etapa 1: habilitar a Amazon GuardDuty

O primeiro passo para usar GuardDuty é habilitá-lo em sua conta. Uma vez ativado, GuardDuty começará imediatamente a monitorar as ameaças à segurança na região atual.

Se você quiser gerenciar GuardDuty descobertas para outras contas em sua organização como GuardDuty administrador, você deve adicionar contas de membros e GuardDuty habilitá-las também.

> **Note**
>
> Se você quiser habilitar a Proteção contra GuardDuty Malware para S3 sem GuardDuty habilitá-la, consulte para ver GuardDuty Proteção contra malware para S3 as etapas.

Standalone account environment

1. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/
2. Selecione a opção Amazon GuardDuty - Todos os recursos.
3. Escolha Começar.
4. Na GuardDuty página Bem-vindo ao, veja os termos do serviço. Escolha Habilitar GuardDuty.

Multi-account environment

> **Important**
>
> Como pré-requisitos para esse processo, você deve estar na mesma organização de todas as contas que deseja gerenciar e ter acesso à conta de AWS Organizations gerenciamento para delegar um administrador dentro da sua organização. GuardDuty Permissões adicionais podem ser necessárias para delegar um administrador. Para obter mais informações, consulte Permissões necessárias para designar uma conta de administrador delegado GuardDuty.

Para designar uma conta de administrador delegado GuardDuty

1. Abra o AWS Organizations console em https://console.aws.amazon.com/organizations/, usando a conta de gerenciamento.
2. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.

   GuardDuty Já está habilitado em sua conta?

   - Se ainda não GuardDuty estiver habilitado, você pode selecionar Começar e designar um administrador GuardDuty delegado na página Bem-vindo ao GuardDuty.
   - Se GuardDuty estiver ativado, você poderá designar um administrador GuardDuty delegado na página Configurações.

3. Insira o ID da AWS conta de doze dígitos da conta que você deseja designar como administrador GuardDuty delegado da organização e escolha Delegar.

> **Note**
>
> Se ainda não GuardDuty estiver habilitado, a designação de um administrador delegado GuardDuty habilitará essa conta na sua região atual.

Para adicionar contas-membro

Esse procedimento abrange a adição de contas de membros a uma conta de administrador GuardDuty delegado por meio AWS Organizations de. Também é possível adicionar membros por convite. Para saber mais sobre os dois métodos de associação de membros em GuardDuty, consulteGerenciando várias contas na Amazon GuardDuty.

1. Faça login na conta de administrador delegado
2. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.
3. No painel de navegação, escolha Configurações e selecione Contas.

   A tabela de contas exibe todas as contas na organização.
4. Selecione as contas que deseja adicionar como membros marcando a caixa de seleção ao lado do ID da conta. Depois, no menu Ação, selecione Adicionar membro.

> **Tip**
>
> Você pode automatizar a adição de novas contas como membros ativando o Auto-enablerecurso; no entanto, isso só se aplica às contas que ingressam na sua organização após a ativação do recurso.

Etapa 2: gerar descobertas de amostra e explorar as operações básicas

Quando GuardDuty descobre um problema de segurança, ele gera uma descoberta. Uma GuardDuty descoberta é um conjunto de dados contendo detalhes relacionados a esse problema de segurança exclusivo. Os detalhes da descoberta podem ser usados para ajudar a investigar o problema.

GuardDuty suporta a geração de amostras de descobertas com valores de espaço reservado, que podem ser usados para testar a GuardDuty funcionalidade e se familiarizar com as descobertas antes de precisar responder a um problema de segurança real descoberto por. GuardDuty Siga o guia abaixo para gerar exemplos de descobertas para cada tipo de descoberta disponível em GuardDuty. Para obter outras formas de gerar exemplos de descobertas, incluindo a geração de um evento de segurança simulado em sua conta, consulteAmostras de descobertas.

Para criar e explorar descobertas de amostra

1. No painel de navegação, selecione Configurações.
2. Na página Configurações, em Amostras de descobertas, escolha Gerar amostras de descobertas.
3. No painel de navegação, escolha Resumo para visualizar os insights sobre as descobertas geradas em seu AWS ambiente. Para obter mais informações sobre os componentes do painel de resumo, consulte Painel de resumo na Amazon GuardDuty.
4. No painel de navegação, selecione Descobertas. As descoberta de amostra são exibidas na página Descobertas atuais com o prefixo [SAMPLE].
5. Selecione uma descoberta na lista para exibir os detalhes dela.

    - Os diversos campos de informações disponíveis podem ser revisados no painel de detalhes da descoberta. Tipos diferentes de descobertas podem ter campos diferentes. Para obter mais informações sobre os campos disponíveis em todos os tipos de descoberta, consulte Detalhes da descoberta. No painel de detalhes, você pode utilizar as seguintes ações:

        - Na parte superior do painel, selecione o ID da descoberta para abrir os detalhes completos do JSON da descoberta. Nesse painel também é possível baixar o arquivo JSON completo. O JSON contém algumas informações adicionais não incluídas na visualização do console e é o formato que outras ferramentas e serviços podem ingerir.
        - Veja a seção Recurso afetado. Em uma descoberta real, as informações aqui ajudarão você a identificar um recurso em sua conta que deve ser investigado e incluirão links para os recursos apropriados Console de gerenciamento da AWS para uso.
        - Selecione os ícones de lupa + ou - para criar um filtro inclusivo ou exclusivo para esse detalhe. Para obter mais informações sobre os filtros de descobertas, consulte Filtrando descobertas em GuardDuty.
6. Arquive todas as suas descobertas de amostra

    a. Selecione todas as descobertas marcando a caixa de seleção na parte superior da lista.

b. Desmarque todas as descobertas que você deseja manter.

c. Selecione o menu Ações e, em seguida, selecione Arquivar para ocultar as descobertas de amostra.

> **Note**
>
> Selecione Atual para visualizar as descobertas arquivadas e, em seguida, Arquivado para alternar a visualização das descobertas.

Etapa 3: Configurar a exportação de GuardDuty descobertas para um bucket do Amazon S3

GuardDuty recomenda definir configurações para exportar descobertas porque permite exportar suas descobertas para um bucket do S3 para armazenamento indefinido além do período de retenção de 90 dias. GuardDuty Isso permite que você mantenha registros das descobertas ou acompanhe problemas em seu AWS ambiente ao longo do tempo. GuardDuty criptografa os dados das descobertas em seu bucket do S3 usando AWS Key Management Service ()AWS KMS key. Para definir as configurações, você deve dar GuardDuty à permissão uma chave KMS. Para obter detalhes das etapas, consulte Exportar as descobertas geradas para bucket do Amazon S3.

Para exportar GuardDuty descobertas para o bucket do Amazon S3

1. Anexar política à chave do KMS

   a. Faça login no console Console de gerenciamento da AWS e abra o AWS Key Management Service (AWS KMS) em https://console.aws.amazon.com/kms.

   b. Para alterar o Região da AWS, use o seletor de região no canto superior direito da página.

   c. No painel de navegação, escolha Chaves gerenciadas pelo cliente.

   d. Selecione uma chave do KMS existente ou execute as etapas para Criar uma chave do KMS de criptografia simétrica no Guia do desenvolvedor do AWS Key Management Service .

      A região da sua chave do KMS e do bucket do Amazon S3 deve ser a mesma.

      Copie o ARN da chave em um bloco de notas para uso nas etapas posteriores.

e. Na seção Política de chave da sua chave do KMS, escolha Editar. Se Mudar para visualização da política for exibido, selecione-o para exibir a Política de chave e, em seguida, escolha Editar.

f. Copie o seguinte bloco de política para sua política de chave do KMS:

```
{
    "Sid": "AllowGuardDutyKey",
    "Effect": "Allow",
    "Principal": {
        "Service": "guardduty.amazonaws.com"
    },
    "Action": "kms:GenerateDataKey",
    "Resource": "KMS key ARN",
    "Condition": {
        "StringEquals": {
            "aws:SourceAccount": "123456789012",
            "aws:SourceArn":
 "arn:aws:guardduty:Region2:123456789012:detector/SourceDetectorID"
        }
    }
}
```

Edite a política substituindo os seguintes valores que estão formatados *red*no exemplo de política:

1. *KMS key ARN*Substitua pelo Amazon Resource Name (ARN) da chave KMS. Para saber como localizar o ARN da chave, consulte Localizar o ID da chave e o ARN no Guia do desenvolvedor do AWS Key Management Service .
2. *123456789012*Substitua pelo Conta da AWS ID que possui a GuardDuty conta que exporta as descobertas.
3. *Region2*Substitua pelo Região da AWS local onde as GuardDuty descobertas são geradas.
4. *SourceDetectorID*Substitua pela `detectorID` da GuardDuty conta na região específica em que as descobertas foram geradas.

   Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no https://console.aws.amazon.com/guardduty/console ou execute a ListDetectorsAPI.

2. Anexar política ao bucket do Amazon S3

   Se você ainda não tem um bucket do Amazon S3 para o qual deseja exportar essas descobertas, consulte Criação de um bucket no Guia do usuário do Amazon S3.

   a. Execute as etapas em Para criar ou editar uma política de bucket no Guia do usuário do Amazon S3, até que a página Editar política de bucket seja exibida.

   b. O exemplo de política mostra como conceder GuardDuty permissão para exportar descobertas para seu bucket do Amazon S3. Caso altere o caminho depois de configurar a exportação de descobertas, você deve modificar a política para conceder permissão para o novo local.

      Copie a política de exemplo a seguir e cole-a no Editor de políticas do bucket.

      Se você adicionou a declaração de política antes da declaração final, adicione uma vírgula antes de adicionar essa declaração. Certifique-se de que a sintaxe JSON da sua política de chaves do KMS seja válida.

      Exemplo de política de bucket do S3

      JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "Allow GetBucketLocation",
            "Effect": "Allow",
            "Principal": {
                "Service": "guardduty.amazonaws.com"
            },
            "Action": "s3:GetBucketLocation",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "123456789012",
                    "aws:SourceArn": "arn:aws:guardduty:us-
east-2:123456789012:detector/SourceDetectorID"

                }
            }
```

```
        },
        {
            "Sid": "Allow PutObject",
            "Effect": "Allow",
            "Principal": {
                "Service": "guardduty.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket[optional
 prefix]/*",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "123456789012",
                    "aws:SourceArn": "arn:aws:guardduty:us-
east-2:123456789012:detector/SourceDetectorID"

                }
            }
        },
        {
            "Sid": "Deny unencrypted object uploads",
            "Effect": "Deny",
            "Principal": {
                "Service": "guardduty.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket[optional
 prefix]/*",
            "Condition": {
                "StringNotEquals": {
                    "s3:x-amz-server-side-encryption": "aws:kms"
                }
            }
        },
        {
            "Sid": "Deny incorrect encryption header",
            "Effect": "Deny",
            "Principal": {
                "Service": "guardduty.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket[optional
 prefix]/*",
            "Condition": {
```

```
                "StringNotEquals": {
                "s3:x-amz-server-side-encryption-aws-kms-key-id":
 "arn:aws:kms:us-east-2:111122223333:key/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111"
                }
            }
        },
        {
            "Sid": "Deny non-HTTPS access",
            "Effect": "Deny",
            "Principal": "*",
            "Action": "s3:*",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket[optional
 prefix]/*",
            "Condition": {
                "Bool": {
                    "aws:SecureTransport": "false"
                }
            }
        }
    ]
}
```

c. Edite a política substituindo os seguintes valores que estão formatados *red*no exemplo de política:

1. *Amazon S3 bucket ARN*Substitua pelo nome de recurso da Amazon (ARN) do bucket do Amazon S3. Você pode encontrar o ARN do bucket na página Editar política do bucket no https://console.aws.amazon.com/s3/console.
2. *123456789012*Substitua pelo Conta da AWS ID que possui a GuardDuty conta que exporta as descobertas.
3. *Region2*Substitua pelo Região da AWS local onde as GuardDuty descobertas são geradas.
4. *SourceDetectorID*Substitua pela `detectorID` da GuardDuty conta na região específica em que as descobertas foram geradas.

   Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no https://console.aws.amazon.com/guardduty/console ou execute a ListDetectorsAPI.

5. Substitua *[optional prefix]* parte do valor do *S3 bucket ARN/[optional prefix]* espaço reservado por um local de pasta opcional para o qual você deseja exportar as descobertas. Para obter mais informações sobre ouso de prefixos, consulte Organizando objetos usando prefixos no Guia de usuário do Amazon S3.

   Quando você fornece um local de pasta opcional que ainda não existe, GuardDuty criará esse local somente se a conta associada ao bucket do S3 for a mesma que a conta que exporta as descobertas. Se você exportar descobertas para um bucket do S3 que pertence a outra conta, o local da pasta já deve existir.

6. *KMS key ARN*Substitua pelo Amazon Resource Name (ARN) da chave KMS associada à criptografia das descobertas exportadas para o bucket do S3. Para saber como localizar o ARN da chave, consulte Localizar o ID da chave e o ARN no Guia do desenvolvedor do AWS Key Management Service .

3. Etapas no GuardDuty console

   a. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.

   b. No painel de navegação, selecione Configurações.

   c. Na página Configurações, em Opções de exportação de descobertas, para o bucket do S3, escolha Configurar agora (ou Editar, conforme necessário).

   d. Para o ARN do bucket do S3, insira o **`bucket ARN`** para o qual você deseja enviar as descobertas. Para visualizar o ARN do bucket, consulte Visualização das propriedades de um bucket do S3 no Guia do usuário do Amazon S3.

   e. Para o ARN da chave do KMS, insira o **`key ARN`**. Para localizar o ARN da chave, consulte Localizar o ID da chave e o ARN no Guia do desenvolvedor do AWS Key Management Service .

   f. Escolha Salvar.

Etapa 4: configurar alertas de GuardDuty busca por meio do SNS

GuardDuty se integra à Amazon EventBridge, que pode ser usada para enviar dados de descobertas para outros aplicativos e serviços para processamento. Com EventBridge você pode usar GuardDuty as descobertas para iniciar respostas automáticas às suas descobertas conectando eventos de busca a destinos como AWS Lambda funções, automação do Amazon EC2 Systems Manager, Amazon Simple Notification Service (SNS) e muito mais.

Neste exemplo, você criará um tópico do SNS para ser o alvo de uma EventBridge regra e, em seguida, usará EventBridge para criar uma regra que capture dados de descobertas. GuardDuty A regra resultante encaminha os detalhes da descoberta para um endereço de e-mail. Para saber como você pode enviar descobertas para o Slack ou o Amazon Chime e também modificar os tipos de descobertas para os quais os alertas são enviados, consulte Configurar um tópico e um endpoint do Amazon SNS.

Para criar um tópico do SNS para seus alertas de descobertas

1. Abra o console do Amazon SNS em https://console.aws.amazon.com/sns/v3/home.
2. No painel de navegação, escolha Tópicos.
3. Selecione Criar tópico.
4. Em Tipo, selecione Padrão.
5. Em Nome, digite **`GuardDuty`**.
6. Selecione Criar tópico. A seção Detalhes do novo tópico será aberta.
7. Na seção Inscrições, escolha Criar inscrição.
8. Em Protocolo, escolha E-mail.
9. Para Endpoint, insira o endereço de e-mail que deve receber as notificações.
10. Selecione Criar assinatura.

    É necessário confirmar a assinatura por e-mail após a criação da assinatura.
11. Para conferir se há uma mensagem de assinatura, acesse sua caixa de entrada de e-mail e, na mensagem de assinatura, escolha Confirmar assinatura.

> **Note**
>
> Para conferir o status do e-mail de confirmação, acesse o console do SNS e escolha Assinaturas.

Para criar uma EventBridge regra para capturar GuardDuty descobertas e formatá-las

1. Abra o EventBridge console em https://console.aws.amazon.com/events/.
2. No painel de navegação, em Barramentos, selecione Regras.
3. Escolha Create rule.

4. Insira um nome e uma descrição para a regra.

   Uma regra não pode ter o mesmo nome que outra na mesma Região e barramento de eventos.
5. Para Barramento de eventos, verifique se o padrão está selecionado e Habilitar a regra nos barramentos de eventos selecionados está ligado.
6. Para Tipo de regra, escolha Regra com padrão de evento.
7. Escolha Próximo.
8. Na página Criar padrão de evento, em Origem do evento, escolha AWS eventos ou eventos de EventBridge parceiros.
9. Na seção Padrão de evento, em Método de criação, escolha Usar formulário padrão.
10. Em Fonte do evento, selecione Serviços da AWS .
11. Em Serviço da AWS , escolha GuardDuty.
12. Em Tipo de evento, escolha GuardDutyEncontrar.
13. Escolha Próximo.
14. Em Tipos de destino, escolha Serviço da AWS .
15. Em Select a target (Selecionar um destino), escolha SNS topic (Tópico do SNS). Em Local de destino, escolha Destino nesta conta. Em Tópico, escolha o nome do tópico do SNS que você criou anteriormente.
16. Expanda Additional settings (Configurações adicionais). Em Configurar entrada do destino, escolha Transformador de entrada.

    Adicionar um transformador de entrada formata os dados de localização JSON enviados GuardDuty em uma mensagem legível por humanos.
17. Escolha Configurar o transformador de entrada.
18. Na seção Transformador de entrada de destino, em Caminho de entrada, cole este código:

```
{
  "severity": "$.detail.severity",
  "Finding_ID": "$.detail.id",
  "Finding_Type": "$.detail.type",
  "region": "$.region",
  "Finding_Description": "$.detail.description"
}
```

19. Para formatar o e-mail, em Modelo, cole o código a seguir. Ao EventBridge entregar cada descoberta, o transformador de entrada preenche os valores entre colchetes angulares, como `<severity>` e`<Finding_ID>`, do caminho de entrada, para que você não precise substituí-los.

```
{"message":"You have a severity <severity> GuardDuty finding type <Finding_Type> in
 the <region> Region.\n\nFinding Description:\n<Finding_Description>\n\nFor more
 details open the GuardDuty console at https://console.aws.amazon.com/guardduty/
home?region=<region>#/findings?search=id%3D<Finding_ID>"}
```

> **Important**
>
> Forneça o modelo como um objeto JSON de linha única, com a mensagem encapsulada em uma chave`message`, como mostrado no exemplo anterior. Use \n para adicionar quebras de linha.
> GuardDuty campos de busca como os que `description` podem conter caracteres de controle sem escape, incluindo novas linhas. Não use nenhum dos seguintes formatos de modelo:
>
> - Uma string sem aspas
> - Um modelo de várias linhas que usa cadeias de caracteres separadas entre aspas em linhas separadas
>
> Com esses formatos, o valor substituído pode produzir JSON inválido. EventBridge em seguida, rejeita o evento e não entrega a notificação.

> **Note**
>
> As assinaturas de e-mail recebem a saída do modelo como está, então o e-mail mostra o objeto `message` JSON e as quebras de linha aparecem como. \n Para notificações formatadas, entregue o tópico do Amazon SNS ao Amazon Q Developer em aplicativos de bate-papo (Slack ou Amazon Chime) ou use uma função Lambda como destino.

20. Escolha Confirmar.
21. Escolha Próximo.

22. (Opcional) Insira uma ou mais tags para a regra. Para obter mais informações, consulte as EventBridge tags da Amazon no Guia EventBridge do usuário da Amazon.
23. Escolha Próximo.
24. Analise os detalhes da regra e selecione Criar regra.
25. (Opcional) Teste sua nova regra gerando descobertas de exemplo com o processo na Etapa 2. Você receberá um e-mail para cada descoberta de amostra gerada.

Próximas etapas

Ao continuar usando GuardDuty, você entenderá os tipos de descobertas que são relevantes para o seu ambiente. Sempre que receber uma nova descoberta, você pode encontrar informações, incluindo recomendações de remediação sobre essa descoberta, selecionando Saiba mais na descrição da descoberta no painel de detalhes da descoberta ou pesquisando o nome da descoberta em GuardDuty tipos de descoberta.

Os recursos a seguir ajudarão você a se ajustar GuardDuty para que possam fornecer as descobertas mais relevantes para seu AWS ambiente:

- Para classificar facilmente as descobertas com base em critérios específicos, como ID da instância, ID da conta, nome do bucket do S3 e muito mais, você pode criar e salvar filtros nele GuardDuty. Para obter mais informações, consulte Filtrando descobertas em GuardDuty.
- Se você estiver recebendo descobertas sobre o comportamento esperado em seu ambiente, poderá arquivar automaticamente as descobertas com base nos critérios definidos com as regras de supressão.
- Para evitar que descobertas sejam geradas a partir de um subconjunto de IPs confiáveis ou para que os IPs de GuardDuty monitoramento estejam fora do escopo normal de monitoramento, você pode configurar listas de IPs confiáveis e de ameaças.

GuardDuty fontes de dados fundamentais

GuardDuty usa as fontes de dados básicas para detectar a comunicação com domínios e endereços IP maliciosos conhecidos e identificar comportamentos potencialmente anômalos e atividades não autorizadas. Enquanto estão em trânsito dessas fontes para GuardDuty, todos os dados de registro são criptografados. GuardDuty extrai vários campos dessas fontes de registros para criação de perfil e detecção de anomalias e, em seguida, descarta esses registros.

Quando você ativa GuardDuty pela primeira vez em uma região, há um teste gratuito de 30 dias que inclui a detecção de ameaças para todas as fontes de dados fundamentais. Durante esse teste gratuito, você pode monitorar um uso mensal estimado dividido em cada fonte de dados fundamental. Como conta de GuardDuty administrador delegado, você pode ver o custo estimado de uso mensal detalhado por cada conta membro que pertence à sua organização e foi ativada GuardDuty. Após o término do teste de 30 dias, você poderá usar AWS Billing para obter informações sobre o custo de uso.

Não há custo adicional ao GuardDuty acessar os eventos e registros dessas fontes de dados fundamentais.

Depois de habilitar o GuardDuty seu Conta da AWS, ele começa automaticamente a monitorar as fontes de registro explicadas nas seções a seguir. Você não precisa habilitar mais nada para começar GuardDuty a analisar e processar essas fontes de dados para gerar descobertas de segurança associadas.

Tópicos

- AWS CloudTrail eventos de gerenciamento
- Logs de fluxo da VPC
- Logs de consultas de DNS do Route53 Resolver

AWS CloudTrail eventos de gerenciamento

AWS CloudTrail fornece um histórico de chamadas de AWS API para sua conta, incluindo chamadas de API feitas usando o Console de gerenciamento da AWS, os AWS SDKs, as ferramentas de linha de comando e determinados AWS serviços. CloudTrail também ajuda a identificar quais usuários e contas invocaram AWS APIs para serviços compatíveis CloudTrail, o endereço IP de origem de onde as chamadas foram invocadas e a hora em que as chamadas foram invocadas. Para obter mais informações, consulte O que é o AWS CloudTrail no Guia do usuário do AWS CloudTrail .

GuardDuty monitora eventos CloudTrail de gerenciamento, também conhecidos como eventos do plano de controle. Esses eventos fornecem uma visão das operações de gerenciamento que são realizadas com os recursos em seu Conta da AWS.

Veja a seguir exemplos de eventos de CloudTrail gerenciamento que GuardDuty monitoram:

- Configuração da segurança (operações da API `AttachRolePolicy` do IAM)
- Configuração de regras para roteamento de dados (por exemplo, operações de API `CreateSubnet` do Amazon EC2)
- Configurando o registro (operações de AWS CloudTrail `CreateTrail` API)

Quando você ativa GuardDuty, ele começa a consumir eventos CloudTrail de gerenciamento diretamente CloudTrail por meio de um fluxo de eventos independente e duplicado e analisa seus CloudTrail registros de eventos.

GuardDuty não gerencia seus CloudTrail eventos nem afeta suas CloudTrail configurações existentes. Da mesma forma, suas CloudTrail configurações não afetam a forma como GuardDuty consome e processa os registros de eventos. Para gerenciar o acesso e a retenção de seus CloudTrail eventos, use o console CloudTrail de serviço ou a API. Para obter mais informações, consulte Visualização de eventos com histórico de CloudTrail eventos no Guia AWS CloudTrail do usuário.

Como GuardDuty manuseia AWS CloudTrail eventos globais

Para a maioria dos AWS serviços, os CloudTrail eventos são registrados no Região da AWS local em que são criados. Para serviços globais como AWS Identity and Access Management (IAM), AWS Security Token Service (AWS STS), Amazon Simple Storage Service (Amazon S3), Amazon e CloudFront Amazon Route 53 (Route 53), os eventos são gerados somente na região em que ocorrem, mas têm um significado global.

Quando GuardDuty consome eventos de serviço CloudTrail global (GSE) com valor de segurança, como configurações de rede ou permissões de usuário, ele replica esses eventos e os processa em cada região em que você ativou. GuardDuty Esse comportamento ajuda a GuardDuty manter perfis de usuário e função em cada região, o que é vital para detectar eventos anômalos.

> **Note**
>
> Para descobertas geradas a partir desses eventos de serviço global, o valor da região na descoberta pode ser diferente da região em que a detecção é GuardDuty criada. Por

exemplo, uma descoberta pode ser exibida `us-east-1` como a Região, mesmo que GuardDuty crie a detecção em uma região diferente.

Recomendamos que você ative GuardDuty todos os Regiões da AWS disponíveis em seu Conta da AWS. Mesmo que você não tenha recursos implantados em determinadas regiões, GuardDuty a ativação ajuda a proteger sua conta contra possíveis ameaças. Os agentes de ameaças podem potencialmente lançar ataques por meio de serviços globais (como IAM ou Amazon CloudFront). AWS STS Eles podem tentar criar recursos não autorizados para explorar regiões onde você tem presença limitada. GuardDuty processa eventos de serviço globais em todas as regiões em que você ativou o serviço, incluindo regiões padrão e opcionais. Isso ajuda a GuardDuty detectar atividades potencialmente suspeitas em sua região Conta da AWS, incluindo regiões nas quais você não usa recursos ativamente.

Logs de fluxo da VPC

O atributo Logs de fluxo da VPC da Amazon VPC captura informações sobre o tráfego de IP que entra e sai de interfaces de rede anexadas a instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em seu ambiente da AWS .

Quando você ativa GuardDuty, ele imediatamente começa a analisar os dados de log de fluxo da VPC das instâncias do Amazon EC2 em sua conta. GuardDuty consome esses dados por meio de um fluxo independente e duplicado de registros de fluxo. Você não precisa criar ou configurar registros de fluxo de VPC na sua conta GuardDuty para acessar esses dados. Esse processo não afeta nenhuma das suas configurações de log de fluxo existentes.

Proteção do Lambda

A Proteção Lambda é um aprimoramento opcional da Amazon. GuardDuty Atualmente, o Monitoramento de atividades de rede do Lambda inclui registros de fluxo do Amazon VPC de todas as funções do Lambda para sua conta, mesmo aqueles que não usam redes VPC. Para proteger sua função Lambda de possíveis ameaças à segurança, você precisará configurar a Proteção Lambda em sua conta. GuardDuty Para obter mais informações, consulte Proteção do Lambda.

GuardDuty Monitoramento de execução

Quando o agente GuardDuty de segurança é implantado em uma instância do Amazon EC2 e recebe eventos de tempo de execução dela GuardDuty , Conta da AWS você não cobra pela análise dos logs de fluxo de VPC dessa instância. Isso evita custos duplos de uso.

GuardDuty não gerencia seus registros de fluxo nem os torna acessíveis em sua conta. Para gerenciar o acesso e a retenção dos seus registros de fluxo, você precisa configurar o recurso de Logs de fluxo da VPC.

Logs de consultas de DNS do Route53 Resolver

Se você usar resolvedores de AWS DNS para suas instâncias do Amazon EC2 (a configuração padrão), GuardDuty poderá acessar e processar seus registros de consulta de DNS do Route53 Resolver de solicitação e resposta por meio dos resolvedores de DNS internos. AWS Se você usar outro resolvedor de DNS, como OpenDNS ou GoogleDNS, ou se configurar seus próprios resolvedores GuardDuty de DNS, não poderá acessar e processar dados dessa fonte de dados.

Quando você ativa GuardDuty, ele imediatamente começa a analisar seus registros de consulta DNS do Route53 Resolver a partir de um fluxo independente de dados. Esse fluxo de dados é separado dos dados fornecidos pelo atributo Registro em log de consultas do Resolvedor do Route 53. A configuração desse recurso não afeta a GuardDuty análise.

> **Note**
>
> GuardDuty não oferece suporte ao monitoramento de registros de DNS para instâncias do Amazon EC2 que são AWS Outposts iniciadas porque Amazon Route 53 Resolver o recurso de registro de consultas não está disponível nesse ambiente.

GuardDuty Detecção estendida de ameaças

GuardDuty A Detecção Estendida de Ameaças detecta automaticamente ataques em vários estágios que abrangem fontes de dados, vários tipos de AWS recursos e tempo, em um. Conta da AWS Com esse recurso, GuardDuty concentra-se na sequência de vários eventos que ele observa monitorando diferentes tipos de fontes de dados. A Detecção Estendida de Ameaças correlaciona esses eventos para identificar cenários que se apresentam como uma ameaça potencial ao seu AWS ambiente e, em seguida, gera uma descoberta da sequência de ataque.

Tópicos

- Exemplos de cenários de ameaças com sequência de ataque
- Como funciona
- Habilitação de planos de proteção para maximizar a detecção de ameaças
- Detecção estendida de ameaças no GuardDuty console
- Noções básicas e gerenciamento de descobertas de sequências de ataques
- Recursos adicionais do

Exemplos de cenários de ameaças com sequência de ataque

A Detecção Estendida de Ameaças abrange cenários de ameaças que envolvem comprometimento relacionado ao uso indevido de AWS credenciais, tentativas de comprometimento de dados em buckets do Amazon S3 e comprometimento de recursos de contêineres e Kubernetes em clusters do Amazon EKS. Uma única descoberta pode abranger uma sequência de ataque inteira. Por exemplo, a lista a seguir descreve os cenários que GuardDuty podem detectar:

Exemplo 1: AWS credenciais e comprometimento de dados do bucket do Amazon S3

- Um agente de ameaça obtendo acesso não autorizado a uma workload computacional.
- O ator então executa uma série de ações, como escalonamento de privilégios e estabelecimento de persistência.
- Finalmente, o ator exfiltra dados de um recurso do Amazon S3.

Exemplo 2 – comprometimento do cluster do Amazon EKS

- Um agente de ameaça tenta explorar uma aplicação de contêiner dentro de um cluster do Amazon EKS.

- O ator usa esse contêiner comprometido para obter tokens de conta de serviço privilegiada.
- O ator então aproveita esses privilégios elevados para acessar segredos confidenciais do Kubernetes ou recursos da AWS por meio de identidades de pods.

Devido à natureza dos cenários de ameaças associados, GuardDuty considera todos Tipos de descoberta de sequência de ataque como críticos.

O vídeo a seguir mostra como você pode usar a Detecção de Ameaças Avançada.

Demonstração de detecção GuardDuty estendida de ameaças da

Como funciona

Quando você ativa a Amazon GuardDuty em sua conta em um determinado local Região da AWS, a Detecção Estendida de Ameaças também é ativada por padrão. Não há custo adicional associado ao uso da Detecção de Ameaças Avançada. Por padrão, ela correlaciona eventos em todas as Fontes de dados fundamentais. No entanto, quando você ativa mais planos de GuardDuty proteção, como S3 Protection, EKS Protection e Runtime Monitoring, isso abrirá outros tipos de detecções de sequência de ataque ao ampliar a variedade de fontes de eventos. Isso potencialmente ajudará com uma análise de ameaças mais abrangente e com uma melhor detecção das sequências de ataque.

Para obter mais informações, consulte Habilitação de planos de proteção para maximizar a detecção de ameaças.

GuardDuty correlaciona vários eventos, incluindo atividades e GuardDuty descobertas da API. Esses eventos são chamados de Sinais. Às vezes, pode haver eventos em seu ambiente que, por si só, não se apresentam como uma clara ameaça potencial. GuardDuty os chama de sinais fracos. Com a Detecção Estendida de Ameaças, GuardDuty identifica quando uma sequência de várias ações se alinha a uma atividade potencialmente suspeita e gera uma sequência de ataque encontrada em sua conta. Essas várias ações podem incluir sinais fracos e GuardDuty descobertas já identificadas em sua conta.

> **Note**
>
> Ao correlacionar eventos para sequências de ataque, a Detecção de Ameaças Avançada não considera as descobertas arquivadas, incluindo aquelas descobertas que são automaticamente arquivadas devido a Regras de supressão. Esse comportamento garante que somente sinais ativos e relevantes contribuam para a detecção da sequência de ataque. Para garantir que você não seja afetado por isso, revise as regras de supressão existentes na sua conta. Para obter mais informações, consulte Usando regras de supressão com a Detecção de Ameaças Avançada.

GuardDuty também foi projetado para identificar possíveis comportamentos de ataque em andamento ou recentes (dentro de um período contínuo de 24 horas) em sua conta. Por exemplo, um ataque pode começar quando um ator obtém acesso não intencional a uma workload computacional. O ator então executaria uma série de etapas, incluindo enumeração, aumento de privilégios e exfiltração de credenciais. AWS Essas credenciais poderiam ser usadas para comprometimento adicional ou acesso malicioso aos dados.

Habilitação de planos de proteção para maximizar a detecção de ameaças

A Detecção Estendida de Ameaças é ativada automaticamente para todas as GuardDuty contas, avaliando por padrão os sinais de todos os planos de proteção habilitados na conta. GuardDuty As fontes de dados fundamentais fornecem sinais importantes para várias detecções de sequências de ataque. Por exemplo, com a detecção básica de ameaças, GuardDuty pode identificar uma possível sequência de ataque a partir da atividade de descoberta de privilégios do IAM nas APIs do Amazon

S3 e detectar alterações subsequentes no plano de controle do S3, como mudanças que tornam a política de recursos do bucket mais permissiva. No entanto, outras sequências de ataque exigem sinais avançados que só estão disponíveis em planos de proteção avançados, como monitoramento de tempo de execução, proteção S3 e monitoramento de registros de auditoria EKS.

Tópicos

- Detecção de sequências de ataque em clusters do Amazon EKS
- Detecção de sequências de ataque nos buckets do Amazon S3
- Detecção de sequências de ataque em clusters do Amazon ECS
- Detecção de sequências de ataque em grupos de instâncias do Amazon EC2
- Detecção de sequências de ataque envolvendo cargas de trabalho de IA

Detecção de sequências de ataque em clusters do Amazon EKS

GuardDuty correlacionou vários sinais de segurança entre os registros de auditoria do EKS, o comportamento dos processos em tempo de execução e a atividade AWS da API para detectar padrões de ataque sofisticados. Para se beneficiar da Detecção de Ameaças Avançada para EKS, você deve habilitar pelo menos um desses recursos – Proteção do EKS ou Monitoramento de Runtime (com o complemento do EKS). A Proteção do EKS monitora as atividades do ambiente de gerenciamento por meio de logs de auditoria, enquanto o Monitoramento de Runtime observa os comportamentos nos contêineres.

Para uma cobertura máxima e uma detecção abrangente de ameaças, GuardDuty recomenda ativar os dois planos de proteção. Juntos, eles criam uma visão completa de seus clusters EKS, permitindo GuardDuty detectar padrões de ataque complexos. Por exemplo, ele pode identificar uma implantação anômala de um contêiner privilegiado (detectada com a Proteção EKS), seguida por tentativas de persistência, mineração criptográfica e criação reversa de shell dentro desse contêiner (detectada com o Runtime Monitoring). GuardDuty representa esses eventos relacionados como um único achado de gravidade crítica, chamado. AttackSequence:EKS/CompromisedCluster Quando você habilita os dois planos de proteção, a descoberta de sequência de ataque abrange os seguintes cenários de ameaça:

- Comprometimento de contêineres que executam aplicações web vulneráveis
- Acesso não autorizado por meio de credenciais mal configuradas
- Tentativas de aumentar os privilégios
- Solicitações de API suspeitas

- Tentativas de acessar dados de forma maliciosa

A lista a seguir fornece detalhes de quando esses planos de proteção dedicados são habilitados individualmente:

Proteção do EKS

A ativação da Proteção EKS permite detectar sequências de ataque envolvendo atividades do plano de controle de cluster do Amazon EKS. GuardDuty Isso permite GuardDuty correlacionar os registros de auditoria do EKS e a atividade AWS da API. Por exemplo, GuardDuty pode detectar uma sequência de ataque em que um ator tenta acessar não autorizadamente os segredos do cluster, modifica as permissões de controle de acesso baseado em funções (RBAC) do Kubernetes e cria pods privilegiados. Para obter informações sobre como habilitar esse plano de proteção, consulte Proteção do EKS.

Monitoramento de Runtime para Amazon EKS

A habilitação do monitoramento de tempo de execução para clusters do Amazon EKS permite GuardDuty aprimorar a detecção da sequência de ataque do EKS com visibilidade em nível de contêiner. Isso ajuda a GuardDuty detectar possíveis processos maliciosos, comportamentos suspeitos em tempo de execução e possível execução de malware. Por exemplo, GuardDuty pode detectar uma sequência de ataque em que um contêiner começa a exibir um comportamento suspeito, como processos de criptomineração ou estabelecer conexões com endpoints maliciosos conhecidos. Para obter informações sobre como habilitar esse plano de proteção, consulte Monitoramento de runtime.

Se você não habilitar a Proteção EKS ou o Monitoramento de Tempo de Execução, não GuardDuty poderá gerar um Tipos de descoberta da Proteção do EKS ou Tipos de descoberta do Monitoramento de runtime. Portanto, não GuardDuty será capaz de detectar sequências de ataque em vários estágios que envolvam descobertas associadas.

Detecção de sequências de ataque nos buckets do Amazon S3

A ativação do S3 Protection oferece GuardDuty a capacidade de detectar sequências de ataque envolvendo tentativas de comprometimento de dados em seus buckets do Amazon S3. Sem o S3 Protection, GuardDuty pode detectar quando sua política de recursos do bucket do S3 se torna excessivamente permissiva. Quando você ativa o S3 Protection, GuardDuty ganha a capacidade de

detectar possíveis atividades de exfiltração de dados que podem ocorrer após seu bucket do S3 se tornar excessivamente permissivo.

Se o S3 Protection não estiver ativado, não GuardDuty será possível gerar indivíduosTipos de descoberta da Proteção do S3. Portanto, não GuardDuty será capaz de detectar sequências de ataque em vários estágios que envolvam descobertas associadas. Para obter informações sobre como habilitar esse plano de proteção, consulte Proteção do S3.

Detecção de sequências de ataque em clusters do Amazon ECS

GuardDuty pode identificar sequências de ataque, como processos maliciosos, conexões com endpoints maliciosos ou comportamentos de mineração de criptomoedas em contêineres ECS. Ao correlacionar diversos sinais entre a atividade da rede, o comportamento do tempo de execução do processo e a atividade AWS da API, é GuardDuty possível identificar padrões de ataque complexos que podem passar despercebidos por detecções individuais e mapear o vetor de ataque completo.

GuardDuty representa esses eventos relacionados como um único achado de gravidade crítica, chamado. `AttackSequence:ECS/CompromisedCluster` A descoberta da sequência de ataque abrange os seguintes cenários de ameaças:

- Comprometimento de contêineres que executam serviços vulneráveis
- Execução não autorizada de ferramentas suspeitas, malware ou processos de criptomineração
- Tentativas de aumentar os privilégios
- Comunicação com endpoints suspeitos

> **Important**
>
> A detecção estendida de ameaças para ECS requer monitoramento de tempo de execução para Fargate ou EC2, dependendo do tipo de infraestrutura do ECS. O Runtime Monitoring observa comportamentos em contêineres do ECS em execução nas instâncias do Fargate e do EC2. O ECS em instâncias gerenciadas do EC2 não é suportado.

Detecção de sequências de ataque em grupos de instâncias do Amazon EC2

GuardDuty pode identificar sequências de ataque que afetam instâncias individuais ou grupos de instâncias que compartilham atributos comuns, como grupos de Auto Scaling, perfis de instâncias do IAM, modelos de execução, CloudFormation pilhas, AMIs ou IDs de VPC. Essas instâncias podem apresentar comportamentos suspeitos, como processos maliciosos, conexões com endpoints maliciosos, mineração de criptomoedas ou uso anormal das credenciais da instância do EC2.

A descoberta da sequência de ataque detecta os seguintes cenários de ameaças:

- Comprometimento de instâncias que executam serviços vulneráveis
- Uso de credenciais de instância do Amazon EC2 obtidas via IMDS de fora da AWS conta para a qual as credenciais foram emitidas
- Use como infraestrutura para ataques como proxy, escaneamento ou negação de serviço
- Execução não autorizada de ferramentas suspeitas, malware ou processos de criptomineração
- Comunicação com endpoints suspeitos

A Detecção Estendida de Ameaças ajuda a identificar essas ameaças. GuardDuty representa esses eventos relacionados como um único achado de gravidade crítica, chamado. `AttackSequence:EC2/CompromisedInstanceGroup`

Para aprimorar a Detecção Estendida de Ameaças para os recursos de detecção do EC2, ative o Runtime Monitoring. A combinação do Foundational GuardDuty, que monitora a atividade da rede, CloudTrail e do Runtime Monitoring, que observa os comportamentos do processo e as chamadas do sistema nas instâncias, fornece uma detecção de ameaças mais abrangente. Esse monitoramento integrado permite GuardDuty detectar sequências de ataque sofisticadas, como acesso não autorizado por meio de credenciais mal configuradas, tentativas de aumento de privilégios e acesso não autorizado a dados confidenciais. Ao correlacionar esses diversos sinais, é GuardDuty possível identificar padrões de ataque complexos que podem passar despercebidos por detecções individuais e mapear o vetor de ataque completo.

Detecção de sequências de ataque envolvendo cargas de trabalho de IA

Ative Proteção da IA para ajudar a GuardDuty detectar sequências de ataque que ameaçam as cargas de trabalho de IA em sua conta. O AI Protection analisa eventos de AWS CloudTrail dados

do Amazon Bedrock e do Amazon SageMaker AI. Ele pode detectar atividades como invocações de modelos anômalos, ataques de coleta de custos e tentativas diretas de injeção imediata.

Para adicionar sinais de suas cargas de trabalho de IA às sequências de AttackSequence:IAM/CompromisedCredentials ataque, você deve ativar a Proteção de IA. GuardDutypode então usar os seguintes tipos de descoberta como sinais de correlação:

- Impact:IAMUser/AnomalousModelInvocation
- Impact:IAMUser/CostHarvesting
- Impact:IAMUser/PromptInjection.Direct

Por exemplo, um agente de ameaças pode usar as mesmas AWS credenciais potencialmente comprometidas para fazer uma invocação anômala do modelo Amazon Bedrock ou Amazon AI. SageMaker GuardDuty pode correlacionar essa invocação com outras ações suspeitas tomadas com essas credenciais. Em seguida, ele os representa como uma única descoberta de sequência de AttackSequence:IAM/CompromisedCredentials ataque. Por si só, as descobertas da AI Protection não geram uma sequência de ataque.

Se o AI Protection não estiver ativado, GuardDuty não será possível gerar um indivíduoTipos de descoberta de proteção de IA. Como resultado, GuardDuty não é possível detectar sequências de ataque em vários estágios que envolvam essas descobertas. Para obter informações sobre como habilitar esse plano de proteção, consulte Proteção da IA.

Detecção estendida de ameaças no GuardDuty console

Por padrão, a página Detecção Estendida de Ameaças no GuardDuty console exibe o Status como Ativado. Com a detecção fundamental de ameaças, o status representa a capacidade de detectar uma GuardDuty possível sequência de ataque envolvendo a atividade de descoberta de privilégios do IAM nas APIs do Amazon S3 e a detecção de alterações subsequentes no plano de controle do S3.

Use as etapas a seguir para acessar a página Detecção Estendida de Ameaças no GuardDuty console:

1. Você pode abrir o GuardDuty console em https://console.aws.amazon.com/guardduty/.
2. No painel de navegação à esquerda, escolha Detecção de Ameaças Avançada.

Essa página fornece detalhes sobre os cenários de ameaças abordados pela Detecção de Ameaças Avançada.

3. Na página Detecção de Ameaças Avançada, veja a seção Planos de proteção relacionados. Se você quiser habilitar planos de proteção dedicados para aprimorar a cobertura de detecção de ameaças na sua conta, selecione a opção Configurar para esse plano de proteção.

Noções básicas e gerenciamento de descobertas de sequências de ataques

As descobertas da sequência de ataque são iguais às outras GuardDuty descobertas em sua conta. Você pode visualizá-los na página Descobertas no GuardDuty console. Para obter mais informações sobre como visualizar descobertas, consulte Página de descobertas no GuardDuty console.

Semelhante a outras GuardDuty descobertas, as descobertas da sequência de ataque também são enviadas automaticamente para a Amazon EventBridge. Com base nas suas configurações, as descobertas de sequência de ataque também são exportadas para um destino de publicação (bucket do Amazon S3). Para definir um novo destino de publicação ou atualizar um existente, consulte Exportar as descobertas geradas para bucket do Amazon S3.

Recursos adicionais do

Veja as seções a seguir para obter uma maior compreensão sobre as sequências de ataque:

- Depois de aprender sobre a Detecção de Ameaças Avançada e as sequências de ataque, você pode gerar exemplos de tipos de descoberta de sequências de ataque seguindo as etapas em Amostras de descobertas.
- Saiba mais sobre o Tipos de descoberta de sequência de ataque.
- Analise as descobertas e explore os detalhes da descoberta associados a Detalhes da descoberta da sequência de ataques.
- Priorize e resolva os tipos de descoberta de sequências de ataque seguindo as etapas dos recursos afetados associados em Correção de descobertas.

Configurando planos de proteção

A página Planos de Proteção no GuardDuty console consolida todas as configurações do plano de proteção em uma única página. Você pode ativar ou desativar planos de proteção, definir configurações de ativação automática para AWS Organizations contas e visualizar estatísticas de contas de membros em um único local.

Visão geral do

A página unificada de Planos de Proteção substitui a necessidade de navegar até as páginas individuais do plano de proteção para configuração. A navegação do console mostra um único link de Planos de Proteção.

A página exibe os planos de proteção na seguinte ordem:

1. Fundamental GuardDuty — Ative ou desative GuardDuty e configure a ativação automática para AWS Organizations contas.
2. Proteção S3 — Monitore eventos de dados do Amazon S3 em busca de possíveis ameaças aos seus dados.
3. Monitoramento de tempo de execução — monitore eventos em nível de sistema operacional para cargas de trabalho EKS, ECS e EC2.
4. Registros de auditoria do EKS — Monitore os registros de auditoria do Amazon EKS em busca de possíveis ameaças aos seus clusters.
5. Proteção do RDS — Monitore a atividade de login do RDS em busca de possíveis ameaças aos seus bancos de dados.
6. Proteção Lambda — Monitore a atividade da rede da função Lambda em busca de possíveis ameaças.

Cada plano de proteção exibe as seguintes informações:

- Status do recurso (ativado ou não ativado)
- Auto-enable status das AWS Organizations contas
- AWS Organizations estatísticas de membros de contas

Configurando todos os planos de proteção

Para configurar planos de proteção na página unificada, use as seguintes etapas:

1. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.
2. No painel de navegação, escolha Planos de proteção.
3. Escolha Configurar todas as habilitações. Todos os contêineres do plano de proteção mudam para o modo de edição.
4. Faça alterações em qualquer um ou em todos os planos de proteção. Para cada plano, você pode ativar ou desativar o recurso e definir a configuração de ativação automática para contas da organização.
5. Escolha Save all. Um modal de confirmação aparece resumindo todas as alterações, incluindo o nome do recurso, o status e o valor de ativação automática para cada plano modificado.
6. Revise as alterações e escolha Confirmar e salvar. Todas as alterações são salvas em lote.

Auto-enable opções

Cada plano de proteção fornece as seguintes opções de ativação automática para contas da organização:

Ativar para todas as contas

Ative o recurso para todas as GuardDuty contas ativas na organização. Isso inclui novas contas que ingressam na organização.

Ativar para novas contas

Isso se aplicará a todas as novas contas quando elas forem adicionadas à organização.

Não habilite automaticamente

O recurso não é ativado automaticamente para contas da organização.

Para o GuardDuty contêiner Foundational, as opções de ativação automática usam palavras AWS Organizations específicas:

- Habilitar para todas as AWS Organizations contas — Ativar GuardDuty para todas as contas ativas em seu AWS Organizations.

- Ativar para novas AWS Organizations contas — Isso se aplicará a todas as novas contas quando elas forem adicionadas à sua AWS Organizations.

Configuração de monitoramento de tempo de execução

O contêiner Runtime Monitoring tem uma estrutura pai-filho com os seguintes subrecursos:

- Monitoramento de tempo de execução (EKS)
- Monitoramento de tempo de execução (ECS)
- Monitoramento de tempo de execução (EC2)

A configuração da infraestrutura de monitoramento de tempo de execução é exibida em uma seção expansível. Essa configuração é necessária para que o Runtime Monitoring for EKS, ECS e EC2 funcione, mas não fornece proteção por si só.

Restrições bidirecionais

Os sub-recursos e a infraestrutura do Runtime Monitoring têm as seguintes relações:

Ativar um subrecurso

Ativa automaticamente a infraestrutura de monitoramento de tempo de execução se ela estiver desativada.

Desativar um subrecurso

Nenhum efeito na infraestrutura de monitoramento de tempo de execução.

Habilite a infraestrutura de monitoramento de tempo

Sem efeito nas sub-características.

Desativar infraestrutura de monitoramento de tempo de execução

Desativa todos os sub-recursos.

Para configurações de ativação automática, as seguintes restrições se aplicam:

Aumente a ativação automática de um subrecurso

A infraestrutura de monitoramento de tempo de execução sempre é igual ao máximo de todos os sub-recursos.

Diminuir a ativação automática de um subrecurso

A infraestrutura de monitoramento de tempo de execução recalcula para o novo máximo de todos os subrecursos.

Ativação automática da infraestrutura de monitoramento de tempo de execução

Sem efeito nas sub-características.

Ativação automática da infraestrutura de monitoramento de menor tempo de execução

Diminui qualquer subrecurso que exceda o novo valor principal para corresponder a ele.

> **Note**
>
> Um aviso aparece quando qualquer subrecurso tem um valor diferente da Infraestrutura de Monitoramento de Tempo de Execução (incompatibilidade de alternância ou ativação automática). Habilitar somente a infraestrutura de monitoramento de tempo de execução coloca você no modo manual sem o gerenciamento automático do agente de segurança. Ative o Runtime Monitoring para EKS, ECS ou EC2 para gerenciar automaticamente o agente de segurança para suas cargas de trabalho.

Estatísticas da organização

Cada contêiner do plano de proteção exibe estatísticas da conta do membro, mostrando quantas contas têm o recurso ativado. Quando as estatísticas da organização ainda não estão disponíveis (por exemplo, nas primeiras 24 horas após a ativação), a página exibe um indicador de status pendente com uma mensagem explicando que as estatísticas estão sendo coletadas.

Integração da página de contas

O botão Editar na seção de ativação automática na página Contas redireciona você para a página Planos de Proteção em vez de abrir o modal de configuração antigo.

GuardDuty Proteção de IA

GuardDuty O AI Protection estende a detecção de GuardDuty ameaças da Amazon às cargas de trabalho de IA incorporadas AWS. Quando você ativa a Proteção de IA, GuardDuty analisa eventos de AWS CloudTrail dados do Amazon Bedrock, Amazon Bedrock AgentCore e Amazon SageMaker AI, junto com AWS CloudTrail eventos de gerenciamento. GuardDuty usa esses dados para detectar atividades potencialmente suspeitas que tenham como alvo os modelos básicos e os aplicativos que os invocam. Quando GuardDuty identifica uma ameaça potencial, ela gera uma ou maisTipos de descoberta de proteção de IA.

Quando você ativa a Proteção de IA, GuardDuty pode detectar os seguintes tipos de ameaças:

- Invocações anômalas dos modelos Amazon Bedrock ou SageMaker Amazon AI que se desviam da linha de base estabelecida para uma identidade ou conta, como invocações de um endereço IP incomum, uma API incomum ou um modelo incomum.
- Ataques de coleta de custos, nos quais um agente de ameaça envia informações computacionalmente caras para um modelo Amazon Bedrock ou Amazon SageMaker AI para aumentar o consumo de tokens e os custos operacionais da conta.
- Tentativas de injeção direta imediata, nas quais um agente da ameaça cria uma solicitação maliciosa para fazer com que um modelo básico ignore suas instruções originais. Essa detecção requer o Amazon Bedrock Guardrails e se aplica somente às cargas de trabalho do Amazon Bedrock.

> **Note**
>
> Os tipos de descoberta que GuardDuty podem ser gerados em e Região da AWS dependem de quais serviços de IA estão disponíveis nessa região:
>
> - Os tipos de Impact:IAMUser/CostHarvesting descoberta Impact:IAMUser/AnomalousModelInvocation e de localização exigem Amazon Bedrock ou Amazon SageMaker AI. Nas regiões em que o Amazon Bedrock não está disponível, GuardDuty gera esses tipos de descoberta somente a partir de invocações do modelo de SageMaker IA da Amazon.
> - O tipo de Impact:IAMUser/PromptInjection.Direct descoberta requer Amazon Bedrock Guardrails. Ele não está disponível em regiões onde o Amazon Bedrock Guardrails não é suportado.

Para ver a lista de regiões em que cada tipo de descoberta é suportado, consulteRegion-specific disponibilidade de recursos.

> **Tip**
>
> Para obter o máximo valor de segurança da proteção de IA, aplique o Amazon Bedrock Guardrails para ataques imediatos em todas as contas da sua organização. AWS Use as políticas do AWS Organizations Amazon Bedrock para gerenciar essas configurações de proteção centralmente. Isso permite uma proteção uniforme em todas as contas com controle e gerenciamento centralizados. Quando uma barreira de proteção de ataque imediata é aplicada, GuardDuty cria resultados imediatos de injeção. Para obter mais informações, consulte Impact:IAMUser/PromptInjection.Direct.

Para detectar ameaças às suas cargas de trabalho de IA, você deve ativar a Proteção de IA em sua GuardDuty conta. Para obter informações sobre como ativar a Proteção de IA, consulte Habilitando a proteção de IA em ambientes com várias contas para ambientes com várias contas ou. Ativando o AI Protection para uma conta independente

Tópicos

- Como funciona a proteção de IA
- Preços da proteção de IA
- Detecções adicionais de ameaças para cargas de trabalho de IA
- Habilitando a proteção de IA em ambientes com várias contas
- Ativando o AI Protection para uma conta independente

Como funciona a proteção de IA

Quando você ativa a Proteção de IA para uma conta ou em toda a sua organização, começa GuardDuty automaticamente a coletar eventos de AWS CloudTrail dados dos serviços de IA nas contas monitoradas. Você não precisa criar uma trilha, ativar o registro de eventos de dados ou fazer alterações em seus aplicativos de IA.

Para coletar os eventos de dados, GuardDuty cria um canal AWS CloudTrail vinculado ao serviço em cada conta monitorada. O canal vinculado ao serviço transmite eventos de AWS CloudTrail dados para Amazon Bedrock, Amazon AgentCore Bedrock e SageMaker Amazon AI, além de recursos de IA GuardDuty relacionados para análise. Porque GuardDuty cria e gerencia esse canal:

- GuardDuty define as configurações de eventos de dados do canal, e o proprietário da conta não pode modificá-las. Isso significa que a detecção de ameaças não depende da configuração ou manutenção de uma trilha pelo proprietário da conta.
- Cada conta monitorada pode confirmar que o canal está ativo no CloudTrail console (em Configurações, Service-linkedcanais) ou chamando a operação da AWS CloudTrail ListChannelsAPI.

GuardDuty usa dois métodos de detecção para gerar descobertas do AI Protection, dependendo do tipo de descoberta:

- Para os tipos Impact:IAMUser/AnomalousModelInvocation e de Impact:IAMUser/CostHarvesting descoberta, GuardDuty usa um modelo de aprendizado de máquina (ML) de detecção de anomalias para analisar os eventos coletados e estabelecer uma linha de base da atividade normal de invocação do modelo para cada identidade do IAM e. Conta da AWS GuardDuty gera uma descoberta quando detecta uma atividade que se desvia significativamente dessa linha de base.
- Para o tipo de Impact:IAMUser/PromptInjection.Direct descoberta, GuardDuty gera uma descoberta quando o Amazon Bedrock Guardrails avalia uma solicitação e detecta um ataque imediato, com base no evento de dados resultante. AWS CloudTrail

Para obter mais informações sobre eventos de AWS CloudTrail dados, consulte Registrar eventos de dados no Guia AWS CloudTrail do usuário.

Preços da proteção de IA

Quando você ativa o GuardDuty AI Protection, GuardDuty cobra pelo volume de eventos de AWS CloudTrail dados que ele analisa, medido em GB. GuardDuty cria o canal vinculado ao serviço sem nenhum CloudTrail custo adicional para você. O custo da coleta desses eventos de dados está incluído no custo de uso do AI Protection. Você também continua incorrendo em custos de uso padrão GuardDuty e de quaisquer outros planos de proteção habilitados. Para ver os preços e exemplos atuais, consulte os GuardDuty preços da Amazon.

Detecções adicionais de ameaças para cargas de trabalho de IA

Além do plano de proteção de IA, os planos Amazon GuardDuty Foundational e Lambda Protection oferecem detecções para ajudar você a proteger e detectar ameaças às cargas de trabalho de IA incorporadas. AWS

O plano GuardDuty Foundational monitora eventos AWS CloudTrail de gerenciamento para detectar atividades suspeitas e maliciosas em cargas de trabalho de IA criadas usando AWS serviços, incluindo Amazon Bedrock e Amazon AI. SageMaker Por exemplo, GuardDuty pode identificar atividades como:

- Remoção incomum da barreira de proteção do Amazon Bedrock
- Uma mudança em uma fonte de dados de treinamento de modelo que pode potencialmente levar a um ataque de envenenamento de dados
- Registro desativado para invocações do modelo Amazon Bedrock que podem indicar tentativas de evitar a detecção
- Instância incomum de notebook ou criação de trabalho de treinamento na Amazon SageMaker AI
- Credenciais extraídas do Amazon Elastic Compute Cloud que podem ter sido usadas para chamar APIs no Amazon Bedrock, Amazon SageMaker AI ou cargas de trabalho de IA autogerenciadas em instâncias do Amazon EC2, clusters do Amazon EKS ou tarefas do Amazon ECS.

GuardDuty O Lambda Protection pode ajudar a detectar possíveis ameaças relacionadas aos agentes do Amazon Bedrock. Isso pode incluir atividades de rede suspeitas, como criptomineração, e comunicação com servidores maliciosos de comando e controle. Essas ameaças podem ser causadas por um ataque à cadeia de suprimentos ou por um aviso complexo.

Habilitando a proteção de IA em ambientes com várias contas

Em um ambiente de várias contas, somente a conta do GuardDuty administrador delegado pode ativar ou desativar a Proteção de IA para as contas dos membros da organização. As contas dos membros não podem modificar essa configuração a partir de suas próprias contas. A conta de GuardDuty administrador delegado gerencia as contas dos membros usando AWS Organizations e pode optar por ativar automaticamente a Proteção de IA para todas as novas contas à medida que elas ingressam na organização. Para obter mais informações sobre ambientes com várias contas, consulte Gerenciamento de várias contas na Amazon. GuardDuty

Ativando o AI Protection para a conta de GuardDuty administrador delegado

Escolha seu método de acesso preferido para ativar a Proteção de IA para a conta de GuardDuty administrador delegado.

Console

1. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.
2. No painel de navegação, escolha Planos de proteção.
3. Escolha Configurar todas as habilitações. Em Proteção de IA, você pode ver o status atual da configuração da Proteção de IA.
4. Execute um destes procedimentos:

   Utilizar Ativar para todas as contas

   - Escolha Habilitar para todas as contas. Isso habilitará o plano de proteção para todas as GuardDuty contas ativas em sua AWS organização, incluindo as novas contas que ingressam na organização.
   - Escolha Salvar.

   Utilizar Configurar contas manualmente

   - Para habilitar o plano de proteção somente para a conta de GuardDuty administrador delegado, escolha Configurar contas manualmente.
   - Escolha Habilitar na seção Conta de GuardDuty administrador delegado (esta conta).
   - Escolha Salvar.

API/CLI

Execute a operação da API UpdateDetector usando seu próprio ID de detector regional e transmitindo o `name` do objeto `features` como `AI_PROTECTION` e `status` como `ENABLED` ou `DISABLED`.

Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no https://console.aws.amazon.com/guardduty/console ou execute a ListDetectorsAPI.

O exemplo a seguir ativa o AI Protection para a conta de GuardDuty administrador delegado. *12abc34d567e8fa901bc2d34e56789f0*Substitua pelo ID do detector da sua conta e *us-east-1* pela região em que você deseja ativar a Proteção de IA.

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
region us-east-1 --features '[{"Name": "AI_PROTECTION", "Status": "ENABLED"}]'
```

Para desativar a Proteção de IA, `ENABLED` substitua por`DISABLED`.

Ativando a proteção de IA para todas as contas de membros ativas existentes

Escolha seu método de acesso preferido para ativar a Proteção de IA para todas as contas de membros ativos existentes na organização.

Console

1. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.

   Certifique-se de usar as credenciais da conta de GuardDuty administrador delegado.
2. No painel de navegação, escolha Planos de proteção.
3. Escolha Configurar todas as habilitações. Em Proteção de IA, na seção Contas de membros ativos, escolha Ações.
4. No menu suspenso Ações, escolha Habilitar para todas as contas-membro ativas existentes.
5. Escolha Salvar.

API/CLI

Para ativar ou desativar seletivamente a Proteção de IA para suas contas de membros, execute a operação da UpdateMemberDetectorsAPI usando a sua própria*detector ID*.

Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no https://console.aws.amazon.com/guardduty/console ou execute a ListDetectorsAPI.

O exemplo a seguir ativa o AI Protection para uma única conta de membro. Para desabilitá-la, substitua `ENABLED` por `DISABLED`. Também é possível passar uma lista de IDs de conta separados por um espaço.

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --account-ids 111122223333 --region us-east-1 --features '[{"Name":
 "AI_PROTECTION", "Status": "ENABLED"}]'
```

Quando o comando é executado com êxito, ele retorna uma lista vazia de`UnprocessedAccounts`. Se houver algum problema ao alterar as configurações do detector de uma conta, a resposta listará esse ID da conta junto com um resumo do problema.

Auto-enable Proteção de IA para novas contas de membros

Escolha seu método de acesso preferido para ativar a Proteção de IA para novas contas que ingressam na sua organização.

No console, a conta de GuardDuty administrador delegado pode ativar automaticamente a Proteção de IA para novas contas de membros usando a página Planos de Proteção ou a página Contas.

Console

1. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.

   Certifique-se de usar as credenciais da conta de GuardDuty administrador delegado.
2. Execute um destes procedimentos:
   - Usando a página Planos de Proteção:
     1. No painel de navegação, escolha Planos de proteção.
     2. Escolha Configurar todas as habilitações.
     3. Em Proteção de IA, escolha Configurar contas manualmente e selecione Ativar automaticamente para novas contas de membros. Essa etapa garante que, sempre que uma nova conta ingressar na sua organização, ative GuardDuty automaticamente a Proteção de IA para essa conta. Somente a conta do GuardDuty administrador delegado da organização pode modificar essa configuração.
     4. Escolha Salvar.
   - Como usar a página Contas:
     1. No painel de navegação, selecione Contas.
     2. Na página Contas, escolha Auto-enablepreferências.

3. Na janela Gerenciar preferências de ativação automática, selecione Ativar para novas contas em Proteção de IA.
4. Escolha Salvar.

API/CLI

Para ativar a Proteção de IA para novas contas de membros, execute a operação da UpdateOrganizationConfigurationAPI usando a sua própria*detector ID*.

Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no https://console.aws.amazon.com/guardduty/console ou execute a ListDetectorsAPI.

O exemplo a seguir ativa o AI Protection para novas contas que ingressam na sua organização. Se você não quiser habilitá-lo para todas as novas contas, `AutoEnable` defina como`NONE`.

```
aws guardduty update-organization-configuration --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --region us-east-1 --auto-enable --features
 '[{"Name": "AI_PROTECTION", "AutoEnable": "NEW"}]'
```

Ativando o AI Protection para uma conta independente

Uma conta independente é responsável pela decisão de ativar ou desativar um plano de proteção em sua AWS conta em uma região específica.

Se sua conta estiver associada a uma conta de GuardDuty administrador por meio de AWS Organizations ou por convite, esta seção não se aplica a você. Para obter informações sobre como gerenciar várias contas, consulte Habilitando a proteção de IA em ambientes com várias contas.

Depois de habilitar o AI Protection, GuardDuty começa a monitorar a atividade de invocação do modelo Amazon Bedrock e Amazon SageMaker AI que ele coleta para sua conta. CloudTrail

Escolha seu método de acesso preferido para ativar a Proteção de IA em sua conta independente.

Console

1. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.
2. No seletor de região no canto superior direito, selecione uma região na qual você deseja ativar a proteção de IA.

3. No painel de navegação, escolha Planos de proteção.
4. Escolha Configurar todas as habilitações. Em Proteção de IA, escolha Ativar para ativar a Proteção de IA.
5. Escolha Salvar tudo e, em seguida, escolha Confirmar e salvar.

API/CLI

Execute a operação da API UpdateDetector usando seu próprio ID de detector regional e transmitindo o `name` do objeto `features` como `AI_PROTECTION` e `status` como `ENABLED`.

Como alternativa, você pode usar o AWS CLI para ativar a Proteção de IA. Execute o comando a seguir e *`12abc34d567e8fa901bc2d34e56789f0`* substitua pelo ID do detector da sua conta e *`us-east-1`* pela região em que você deseja ativar a Proteção de IA.

Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no https://console.aws.amazon.com/guardduty/console ou execute a ListDetectorsAPI.

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
region us-east-1 --features '[{"Name": "AI_PROTECTION", "Status": "ENABLED"}]'
```

Para desativar a Proteção de IA, `ENABLED` substitua por`DISABLED`.

GuardDuty Proteção EKS

> **Note**
>
> Você pode configurar o EKS Protection junto com todos os outros planos de proteção em uma única página no GuardDuty console. Para obter mais informações, consulte Configurando planos de proteção.

O EKS Protection ajuda você a detectar possíveis riscos de segurança nos clusters do Amazon Elastic Kubernetes Service (Amazon EKS) em seu ambiente. AWS Por exemplo, ele ajuda a detectar quando um cluster EKS mal configurado está sendo acessado por um ator não autenticado que tenta coletar segredos ou AWS credenciais do seu cluster. A Proteção EKS usa registros de auditoria do EKS para analisar as atividades de usuários e aplicativos.

Quando você ativa a Proteção EKS, começa GuardDuty automaticamente a monitorar seus clusters do Amazon EKS em busca de possíveis ameaças à segurança. GuardDuty usa seu próprio fluxo independente para coletar e analisar Logs de auditoria do EKS na Proteção EKS — nenhuma configuração adicional é necessária.

Quando GuardDuty detecta uma ameaça potencial com base no monitoramento do registro de auditoria do EKS, ela gera uma descoberta de segurança. Para obter informações sobre os tipos de descoberta que GuardDuty podem ser gerados quando você ativa a Proteção EKS, consulteTipos de descoberta da Proteção do EKS.

> **Note**
>
> Para visualizar os registros de auditoria do EKS em sua conta (opcional), você pode configurar o registro do plano de controle do Amazon EKS para enviar registros de auditoria para o CloudWatch Logs. Essa configuração é separada da Proteção EKS e não é necessária para a capacidade de monitoramento de segurança no GuardDuty.

Avaliação gratuita de 30 dias

- Ao ativar o GuardDuty in an Conta da AWS in an Região da AWS pela primeira vez, você recebe um teste gratuito de 30 dias. Nesse caso, também GuardDuty ativará o EKS Protection, que está incluído no teste gratuito de 30 dias.

- Quando você já estiver usando GuardDuty e decidir ativar o EKS Protection pela primeira vez, sua conta nessa região receberá um teste gratuito de 30 dias do EKS Protection.
- É possível optar por desabilitar a Proteção do EKS em qualquer região a qualquer momento.
- Durante a avaliação gratuita de 30 dias, é possível obter uma estimativa de seus custos de uso para essa conta e região. Após o término do teste gratuito de 30 dias, GuardDuty não desativa automaticamente a Proteção EKS. Nessa região, haverá custos de uso a serem incorridos em sua conta. Para obter mais informações, consulte Monitorando o uso e estimando custos.

Quando você desativa a Proteção do EKS, interrompe GuardDuty imediatamente o monitoramento e a análise dos registros de auditoria do EKS para seus recursos do Amazon EKS.

A Proteção EKS pode não estar disponível em todos os Regiões da AWS locais GuardDuty disponíveis. Para obter mais informações, consulte Region-specific disponibilidade de recursos.

> **Note**
>
> O Monitoramento de runtime do EKS é gerenciado como parte do Monitoramento de runtime. Para obter mais informações, consulte GuardDuty Monitoramento de execução.

Logs de auditoria do EKS na Proteção EKS

Os logs de auditoria do EKS capturam ações sequenciais no cluster do Amazon EKS, incluindo atividades de usuários, aplicativos que usam a API do Kubernetes e o plano de gerenciamento. Os logs de auditoria são um componente de todos os clusters do Kubernetes.

Para obter mais informações, consulte Auditorias na documentação do Kubernetes.

O Amazon EKS permite que os registros de auditoria do EKS sejam ingeridos como Amazon CloudWatch Logs por meio do recurso de registro do plano de controle do EKS. GuardDuty não gerencia o registro do plano de controle do Amazon EKS nem torna os registros de auditoria do EKS acessíveis em sua conta se você não os tiver ativado para o Amazon EKS. Para gerenciar o acesso e a retenção dos logs de auditoria do EKS, é necessário configurar o recurso de log do plano de gerenciamento do Amazon EKS. Para obter mais informações, consulte Habilitar e desabilitar os logs do ambiente de gerenciamento no Guia do usuário da Amazon EKS.

Habilitando a Proteção do EKS em ambientes de várias contas

Em um ambiente de várias contas, somente a conta do GuardDuty administrador delegado tem a opção de ativar ou desativar o recurso EKS Protection; para as contas dos membros em sua organização. As contas GuardDuty dos membros não podem modificar essa configuração em suas contas. A conta de GuardDuty administrador delegado gerencia suas contas de membros usando AWS Organizations. Essa conta de GuardDuty administrador delegado pode optar por ativar automaticamente a Proteção EKS para todas as novas contas à medida que elas ingressam na organização. Para obter mais informações sobre ambientes com várias contas, consulte Gerenciamento de várias contas na Amazon. GuardDuty

Configurando o monitoramento do registro de auditoria do EKS para uma conta de administrador delegado GuardDuty

Escolha seu método de acesso preferido para configurar o EKS Audit Log Monitoring para a conta do GuardDuty administrador delegado.

Console

1. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.
2. No painel de navegação, escolha Planos de proteção.
3. Escolha Configurar todas as habilitações. Em EKS Audit Logs, você pode ver o status atual da configuração do EKS Audit Log Monitoring.
4. Execute um destes procedimentos:

   Como usar a opção Habilitar para todas as contas

   - Escolha Habilitar para todas as contas. Isso habilitará o plano de proteção para todas as GuardDuty contas ativas em sua AWS organização, incluindo as novas contas que ingressam na organização.
   - Escolha Salvar.

   Como usar a opção Configurar contas manualmente

   - Para habilitar o plano de proteção somente para a conta de GuardDuty administrador delegado, escolha Configurar contas manualmente.
   - Escolha Habilitar na seção Conta de GuardDuty administrador delegado (esta conta).

- Escolha Salvar.

API/CLI

Execute a operação da API updateDetector usando seu próprio ID de detector regional e transmitindo o `name` do objeto `features` como `EKS_AUDIT_LOGS` e `status` como `ENABLED` ou `DISABLED`.

Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no https://console.aws.amazon.com/guardduty/console ou execute a ListDetectorsAPI.

Você pode ativar ou desativar o Monitoramento do Registro de Auditoria do EKS executando o AWS CLI comando a seguir. Certifique-se de usar a conta de GuardDuty administrador delegado válida*`detector ID`*.

> **Note**
>
> O código de exemplo a seguir habilita o Monitoramento de logs de auditoria do EKS. Certifique-se de *`12abc34d567e8fa901bc2d34e56789f0`* substituir pela conta `detector-id` do GuardDuty administrador delegado e *`555555555555`* pela conta Conta da AWS do GuardDuty administrador delegado.

Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no https://console.aws.amazon.com/guardduty/console ou execute a ListDetectorsAPI.

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
features '[{"Name": "EKS_AUDIT_LOGS", "Status": "ENABLED"}]'
```

Para desabilitar o Monitoramento de logs de auditoria do EKS, substitua `ENABLED` por `DISABLED`.

Auto-enable Monitoramento do registro de auditoria do EKS para todas as contas dos membros

Escolha seu método de acesso preferido para habilitar o Monitoramento de logs de auditoria do EKS para contas-membro existentes em sua organização.

Console

1. Faça login no Console de gerenciamento da AWS e abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.

   Certifique-se de usar as credenciais da conta de GuardDuty administrador delegado.

2. Execute um destes procedimentos:

   Usando a página Planos de Proteção

   1. No painel de navegação, escolha Planos de proteção.
   2. Escolha Configurar todas as habilitações. Em EKS Audit Logs, você pode ver o status atual do EKS Audit Log Monitoring para contas de membros ativos em sua organização.
   3. Escolha Habilitar para todas as contas. Essa ação habilita automaticamente o Monitoramento de logs de auditoria do EKS para as contas existentes e novas na organização.
   4. Escolha Salvar tudo e, em seguida, escolha Confirmar e salvar.

   > **Note**
   >
   > Pode levar até 24 horas para atualizar a configuração das contas-membro.

   Como usar a página Contas

   1. No painel de navegação, selecione Contas.
   2. Na página Contas, escolha Auto-enableas preferências antes de Adicionar contas por convite.
   3. Na janela Gerenciar preferências de habilitação automática, escolha Habilitar para todas as contas em Monitoramento de logs de auditoria do EKS.
   4. Escolha Salvar.

   Se você não puder usar a opção Habilitar para todas as contas e quiser personalizar a configuração do Monitoramento de logs de auditoria do EKS para contas específicas em sua organização, consulte Habilitar ou desabilitar seletivamente o Monitoramento de logs de auditoria do EKS para contas-membro.

API/CLI

- Para ativar ou desativar seletivamente o EKS Audit Log Monitoring para suas contas de membros, execute a operação da updateMemberDetectorsAPI usando a sua própria*detector ID*.
- O exemplo a seguir mostra como você pode habilitar o Monitoramento de logs de auditoria do EKS para uma única conta-membro. Para desabilitá-la, substitua `ENABLED` por `DISABLED`.

  Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no https://console.aws.amazon.com/guardduty/console ou execute a ListDetectorsAPI.

  ```
  aws guardduty update-member-detectors --detector-
  id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features
   '[{"name": "EKS_AUDIT_LOGS", "status": "ENABLED"}]'
  ```

  > **Note**
  >
  > Também é possível passar uma lista de IDs de conta separados por um espaço.

- Quando o código é executado com êxito, ele retorna uma lista vazia de `UnprocessedAccounts`. Se houver algum problema na alteração das configurações do detector de uma conta, esse ID de conta será listado junto com um resumo do problema.

Habilite o Monitoramento de logs de auditoria do EKS para todas as contas-membro ativas existentes

Escolha seu método de acesso preferido para habilitar o Monitoramento de logs de auditoria do EKS para todas as contas-membro ativas existentes na organização.

Console

1. Faça login no Console de gerenciamento da AWS e abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.

   Faça login usando as credenciais da conta de GuardDuty administrador delegado.
2. No painel de navegação, escolha Planos de proteção.

3. Escolha Configurar todas as habilitações. Em Registros de auditoria do EKS, na seção Contas de membros ativos, escolha Ações.
4. No menu suspenso Ações, escolha Habilitar para todas as contas-membro ativas existentes.
5. Escolha Salvar.

API/CLI

- Para ativar ou desativar seletivamente o EKS Audit Log Monitoring para suas contas de membros, execute a operação da updateMemberDetectorsAPI usando a sua própria*detector ID*.
- O exemplo a seguir mostra como você pode habilitar o Monitoramento de logs de auditoria do EKS para uma única conta-membro. Para desabilitá-la, substitua `ENABLED` por `DISABLED`.

  Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no https://console.aws.amazon.com/guardduty/console ou execute a ListDetectorsAPI.

  ```
  aws guardduty update-member-detectors --detector-
  id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features
   '[{"name": "EKS_AUDIT_LOGS", "status": "ENABLED"}]'
  ```

  > **Note**
  >
  > Também é possível passar uma lista de IDs de conta separados por um espaço.

- Quando o código é executado com êxito, ele retorna uma lista vazia de `UnprocessedAccounts`. Se houver algum problema na alteração das configurações do detector de uma conta, esse ID de conta será listado junto com um resumo do problema.

Auto-enable Monitoramento do registro de auditoria do EKS para contas de novos membros

As contas de membros recém-adicionadas devem ser ativadas GuardDuty antes de selecionar a configuração da verificação de GuardDuty-initiated malware. As contas dos membros gerenciadas por convite podem configurar manualmente a verificação de GuardDuty-initiated malware em suas contas. Para obter mais informações, consulte Step 3 - Accept an invitation.

Escolha seu método de acesso preferido para habilitar o Monitoramento de logs de auditoria do EKS para novas contas que ingressam na sua organização.

Console

A conta de GuardDuty administrador delegado pode ativar o Monitoramento do Registro de Auditoria do EKS para novas contas membros em uma organização, usando o Monitoramento do Registro de Auditoria do EKS ou a página Contas.

Para habilitar automaticamente o Monitoramento de logs de auditoria do EKS para novas contas-membro

1. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.

   Certifique-se de usar as credenciais da conta de GuardDuty administrador delegado.
2. Execute um destes procedimentos:
   - Usando a página Planos de Proteção:
     1. No painel de navegação, escolha Planos de proteção.
     2. Escolha Configurar todas as habilitações. Em Registros de auditoria do EKS, defina a configuração de ativação automática.
     3. Escolha Configurar contas manualmente.
     4. Selecione Habilitar automaticamente para novas contas-membro. Essa etapa garante que sempre que uma nova conta ingressar em sua organização, o Monitoramento de logs de auditoria do EKS seja habilitado automaticamente para sua conta. Somente a conta do GuardDuty administrador delegado da organização pode modificar essa configuração.
     5. Escolha Salvar.
   - Como usar a página Contas:
     1. No painel de navegação, selecione Contas.
     2. Na página Contas, escolha Auto-enablepreferências.
     3. Na janela Gerenciar preferências de habilitação automática, selecione Habilitar para novas contas em Monitoramento de logs de auditoria do EKS.
     4. Escolha Salvar.

API/CLI

- Para ativar ou desativar seletivamente o EKS Audit Log Monitoring para suas novas contas, execute a operação da UpdateOrganizationConfigurationAPI usando a sua própria*detector ID*.
- O exemplo a seguir mostra como você pode habilitar o Monitoramento de logs de auditoria do EKS para os novos membros que ingressarem na sua organização. Também é possível passar uma lista de IDs de conta separados por um espaço.

  Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no https://console.aws.amazon.com/guardduty/console ou execute a ListDetectorsAPI.

```
aws guardduty update-organization-configuration --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --auto-enable --features '[{"Name":
 "EKS_AUDIT_LOGS", "AutoEnable": "NEW"}]'
```

Habilitar ou desabilitar seletivamente o Monitoramento de logs de auditoria do EKS para contas-membro

Escolha seu método de acesso preferido para habilitar ou desabilitar o Monitoramento de logs de auditoria do EKS para contas-membro seletivas em sua organização.

Console

1. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.

   Certifique-se de usar as credenciais da conta de GuardDuty administrador delegado.
2. No painel de navegação, selecione Contas.

   Na página Contas, revise a coluna Monitoramento de logs de auditoria do EKS para ver o status da sua conta-membro.
3. Para habilitar ou desabilitar o Monitoramento de logs de auditoria do EKS

   Selecione uma conta que você deseja configurar para o Monitoramento de logs de auditoria do EKS. Você pode selecionar várias contas ao mesmo tempo. No menu suspenso Editar planos de proteção, escolha Monitoramento de logs de auditoria do EKS e escolha a opção apropriada.

API/CLI

Para ativar ou desativar seletivamente o EKS Audit Log Monitoring para suas contas de membros, invoque a operação da updateMemberDetectorsAPI usando a sua própria. *detector ID*

O exemplo a seguir mostra como você pode habilitar o Monitoramento de logs de auditoria do EKS para uma única conta-membro. Para desabilitá-la, substitua `ENABLED` por `DISABLED`. Também é possível passar uma lista de IDs de conta separados por um espaço.

Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no https://console.aws.amazon.com/guardduty/console ou execute a ListDetectorsAPI.

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --accountids 111122223333 --features '[{"Name": "EKS_AUDIT_LOGS", "Status":
 "ENABLED"}]'
```

Ativando a Proteção do EKS para uma conta independente

Uma conta autônoma é responsável pela decisão de habilitar ou desabilitar um plano de proteção em sua conta AWS em uma Região específica.

Se sua conta estiver associada a uma conta de GuardDuty administrador por meio AWS Organizations ou pelo método de convite, esta seção não se aplica a você. Para obter informações sobre como gerenciar várias contas, consulte Habilitando a Proteção do EKS em ambientes de várias contas.

Depois de ativar a Proteção EKS, GuardDuty começará a monitorar os registros de auditoria do EKS para os clusters do Amazon EKS em sua conta.

Selecione seu método de acesso preferido para configurar a Proteção do EKS para uma conta independente.

Console

1. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.
2. No seletor de Região do canto superior direito, selecione a Região a ser habilitada a Proteção do EKS.

3. No painel de navegação, escolha Planos de proteção.
4. Escolha Configurar todas as habilitações. Em Registros de auditoria do EKS, escolha Ativar para ativar a proteção do EKS.
5. Escolha Salvar tudo e, em seguida, escolha Confirmar e salvar.

API/CLI

- Execute a operação da updateDetectorAPI usando o ID do detector regional da conta do GuardDuty administrador delegado e transmitindo o nome do `features` objeto `EKS_AUDIT_LOGS` e o status como`ENABLED`.

  Como alternativa, você também pode ativar a Proteção EKS executando um comando do AWS CLI . Execute o comando a seguir e *`12abc34d567e8fa901bc2d34e56789f0`* substitua pelo ID do detector da sua conta e *`us-east-1`* pela região em que você deseja ativar a Proteção EKS.

  Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no https://console.aws.amazon.com/guardduty/console ou execute a ListDetectorsAPI.

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
region us-east-1 --features [{"Name" : "EKS_AUDIT_LOGS", "Status" : "ENABLED"}]'
```

GuardDuty Proteção S3

> **Note**
>
> Você pode configurar o S3 Protection junto com todos os outros planos de proteção em uma única página no GuardDuty console. Para obter mais informações, consulte Configurando planos de proteção.

O S3 Protection ajuda você a detectar possíveis riscos de segurança de dados, como exfiltração e destruição de dados, em seus buckets do Amazon Simple Storage Service (Amazon S3). GuardDuty monitora eventos de AWS CloudTrail dados do Amazon S3, que incluem operações de API em nível de objeto para identificar esses riscos em todos os buckets do Amazon S3 em sua conta.

Quando GuardDuty detecta uma ameaça potencial com base no monitoramento de eventos de dados do S3, ela gera uma descoberta de segurança. Para obter informações sobre os tipos de descoberta que GuardDuty podem ser gerados quando você ativa o S3 Protection, consulteGuardDuty Tipos de localização do S3 Protection.

Por padrão, a detecção de ameaças por base inclui o monitoramento AWS CloudTrail eventos de gerenciamento para identificar possíveis ameaças em seus recursos do Amazon S3. Essa fonte de dados é diferente dos eventos de AWS CloudTrail dados do S3, pois ambos monitoram diferentes tipos de atividades em seu ambiente.

Você pode ativar o S3 Protection em uma conta em qualquer região que GuardDuty ofereça suporte a esse recurso. Isso ajudará você a monitorar eventos de CloudTrail dados do S3 nessa conta e região. Depois de habilitar a Proteção do S3, você GuardDuty poderá monitorar totalmente seus buckets do Amazon S3 e gerar descobertas de acesso suspeito aos dados armazenados em seus buckets do S3.

Para usar a Proteção do S3, você não precisa habilitar ou configurar explicitamente o login de eventos de dados do S3 em AWS CloudTrail.

Teste gratuito de 30 dias

A lista a seguir explica como o teste gratuito de 30 dias funcionaria para sua conta:

- Quando você habilita GuardDuty Conta da AWS em uma nova região pela primeira vez, você recebe um teste gratuito de 30 dias. Nesse caso, também GuardDuty habilitará o S3 Protection, que está incluído no teste gratuito.
- Quando você já estiver usando GuardDuty e decidir ativar o S3 Protection pela primeira vez, sua conta nessa região receberá um teste gratuito de 30 dias do S3 Protection.
- É possível optar por desabilitar a Proteção do S3 em qualquer região a qualquer momento.
- Durante o teste gratuito de 30 dias, você pode obter uma estimativa dos custos de uso nessa conta e região. Após o término do teste gratuito de 30 dias, a Proteção do S3 não será desativada automaticamente. Sua conta nessa região começará a incorrer em custos de uso. Para obter mais informações, consulte Monitorando GuardDuty o uso e estimando custos.

AWS CloudTrail eventos de dados para S3

Eventos de dados, também conhecidos como operações do plano de dados, fornecem insights sobre as operações de recurso executadas no recurso ou dentro de um recurso. Muitas vezes, são atividades de grande volume.

Veja a seguir exemplos de eventos de CloudTrail dados para o S3 que GuardDuty podem ser monitorados:

- Operações de API do `GetObject`
- Operações de API do `PutObject`
- Operações de API do `ListObjects`
- Operações de API do `DeleteObject`

Para ter mais informações sobre esses APIs, consulte Referência da API do Amazon Simple Storage Service.

Como GuardDuty usa eventos CloudTrail de dados para o S3

Quando você ativa o S3 Protection, GuardDuty começa a analisar CloudTrail os eventos de dados do S3 de todos os seus buckets do S3 e os monitora em busca de atividades maliciosas e suspeitas. Para obter mais informações, consulte AWS CloudTrail eventos de gerenciamento.

Quando um usuário não autenticado acessa um objeto do S3, isso significa que o objeto do S3 está acessível ao público. Portanto, GuardDuty não processa essas solicitações. GuardDuty

processa as solicitações feitas aos objetos do S3 usando credenciais IAM (AWS Identity and Access Management) ou AWS STS (AWS Security Token Service) válidas.

> **Observação**
>
> Depois de ativar a Proteção do S3, GuardDuty monitora os eventos de dados desses buckets do Amazon S3 que residem na mesma região em que você habilitou. GuardDuty

Se você desativar a Proteção do S3 em sua conta em uma região específica, GuardDuty interromperá o monitoramento de eventos de dados do S3 dos dados armazenados em seus buckets do S3. GuardDuty não gerará mais tipos de descoberta do S3 Protection para sua conta nessa região.

GuardDuty usando eventos CloudTrail de dados para S3 para sequências de ataque

GuardDuty Detecção estendida de ameaças detecta sequências de ataques em vários estágios que abrangem fontes de dados, recursos da AWS e cronogramas fundamentais em uma conta. Quando GuardDuty observa uma sequência de eventos que é indicativa de uma atividade suspeita recente ou em andamento em sua conta, GuardDuty gera a descoberta da sequência de ataque associada.

Por padrão, quando você ativa GuardDuty, a Detecção Estendida de Ameaças também é ativada em sua conta. Esse recurso cobre o cenário de ameaça associado aos eventos CloudTrail de gerenciamento sem custo adicional. No entanto, para usar o Extended Threat Detection em todo o seu potencial, GuardDuty recomenda habilitar o S3 Protection para cobrir cenários de ameaças associados a eventos de CloudTrail dados para o S3.

Depois de habilitar o S3 Protection, GuardDuty cobrirá automaticamente os cenários de ameaças da sequência de ataque, como comprometimento ou destruição de dados, nos quais seus recursos do Amazon S3 possam estar envolvidos.

Habilitando a Proteção do S3 em ambientes de várias contas

Em um ambiente com várias contas, somente a conta do GuardDuty administrador delegado tem a opção de configurar (ativar ou desativar) a Proteção do S3 para as contas dos membros em sua organização. AWS As contas GuardDuty dos membros não podem modificar essa configuração

em suas contas. A conta de GuardDuty administrador delegado gerencia suas contas de membros usando AWS Organizations. A conta de GuardDuty administrador delegado pode optar por ter o S3 Protection ativado automaticamente em todas as contas, somente em novas contas ou em nenhuma conta na organização. Para obter mais informações, consulte Como gerenciar contas com o AWS Organizations.

Habilitando o S3 Protection para conta de administrador delegado GuardDuty

Escolha seu método de acesso preferido para habilitar o S3 Protection para a conta de GuardDuty administrador delegado.

Console

1. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.
2. No painel de navegação, escolha Proteção do S3.
3. Na página Proteção do S3, escolha Editar.
4. Execute um destes procedimentos:

   Como usar a opção Habilitar para todas as contas

   - Escolha Habilitar para todas as contas. Isso habilitará o plano de proteção para todas as GuardDuty contas ativas em sua AWS organização, incluindo as novas contas que ingressam na organização.
   - Escolha Salvar.

   Como usar a opção Configurar contas manualmente

   - Para habilitar o plano de proteção somente para a conta de GuardDuty administrador delegado, escolha Configurar contas manualmente.
   - Escolha Habilitar na seção Conta de GuardDuty administrador delegado (esta conta).
   - Escolha Salvar.

API/CLI

Execute updateDetectorusando o ID do detector da conta do GuardDuty administrador delegado da região atual e transmitindo o `features` objeto `name` como `S3_DATA_EVENTS` e `status` como`ENABLED`.

Como alternativa, você pode configurar o S3 Protection usando o. AWS Command Line Interface Execute o comando a seguir e certifique-se de *12abc34d567e8fa901bc2d34e56789f0* substituí-lo pelo ID do detector da conta de GuardDuty administrador delegado da região atual.

Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no https://console.aws.amazon.com/guardduty/console ou execute a ListDetectorsAPI.

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
features '[{"Name": "S3_DATA_EVENTS", "Status": "ENABLED"}]'
```

Auto-enable Proteção S3 para todas as contas de membros na organização

Escolha seu método de acesso preferido para habilitar o S3 Protection para a conta de GuardDuty administrador delegado.

Console

1. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.

   Faça login com sua conta de administrador.
2. Execute um destes procedimentos:

   Usando a página Proteção do S3

   1. No painel de navegação, escolha Proteção do S3.
   2. Escolha Habilitar para todas as contas. Essa ação habilita automaticamente a Proteção do S3 para contas novas e existentes na organização.
   3. Escolha Salvar.

      > **Note**
      >
      > Pode levar até 24 horas para atualizar a configuração das contas-membro.

   Como usar a página Contas

   1. No painel de navegação, selecione Contas.

2. Na página Contas, escolha Auto-enableas preferências antes de Adicionar contas por convite.
3. Na janela Gerenciar preferências de habilitação automática, escolha Habilitar para todas as contas em Proteção do S3.
4. Escolha Salvar.

Se você não conseguir usar a opção Habilitar para todas as contas, consulte Habilite seletivamente a Proteção do S3 nas contas-membro.

API/CLI

- Para ativar seletivamente o S3 Protection para suas contas de membros, invoque a operação da updateMemberDetectorsAPI usando a sua própria. *`detector ID`*
- O exemplo a seguir mostra como você pode habilitar a Proteção do S3 para uma conta de membro único. Certifique-se de *`12abc34d567e8fa901bc2d34e56789f0`* substituir pela conta `detector-id` do GuardDuty administrador delegado e. *`111122223333`*

  Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no https://console.aws.amazon.com/guardduty/console ou execute a ListDetectorsAPI.

```
aws guardduty update-member-detectors --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features
 '[{"name": "S3_DATA_EVENTS", "status": "ENABLED"}]'
```

> **Note**
>
> Também é possível passar uma lista de IDs de conta separados por um espaço.

- Quando o código é executado com êxito, ele retorna uma lista vazia de `UnprocessedAccounts`. Se houver algum problema na alteração das configurações do detector de uma conta, esse ID de conta será listado junto com um resumo do problema.

Habilite a Proteção do S3 para todas as contas-membro ativas existentes

Escolha seu método de acesso preferido para habilitar a Proteção do S3 para todas as contas-membro ativas existentes em sua organização.

Console

1. Faça login no Console de gerenciamento da AWS e abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.

   Faça login usando as credenciais da conta de GuardDuty administrador delegado.
2. No painel de navegação, escolha Proteção do S3.
3. Na página Proteção do S3, é possível exibir o status atual da configuração. Na seção Contas-membro ativas, escolha Ações.
4. No menu suspenso Ações, escolha Habilitar para todas as contas-membro ativas existentes.
5. Escolha Confirmar.

API/CLI

- Para ativar seletivamente o S3 Protection para suas contas de membros, invoque a operação da updateMemberDetectorsAPI usando a sua própria. *`detector ID`*
- O exemplo a seguir mostra como você pode habilitar a Proteção do S3 para uma conta de membro único. Certifique-se de *`12abc34d567e8fa901bc2d34e56789f0`* substituir pela conta `detector-id` do GuardDuty administrador delegado e. *`111122223333`*

  Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no https://console.aws.amazon.com/guardduty/console ou execute a ListDetectorsAPI.

```
aws guardduty update-member-detectors --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features
 '[{"name": "S3_DATA_EVENTS", "status": "ENABLED"}]'
```

> **Note**
>
> Também é possível passar uma lista de IDs de conta separados por um espaço.

- Quando o código é executado com êxito, ele retorna uma lista vazia de `UnprocessedAccounts`. Se houver algum problema na alteração das configurações do detector de uma conta, esse ID de conta será listado junto com um resumo do problema.

Auto-enable Proteção S3 para contas de novos membros

Selecione seu método de acesso preferido para habilitar a Proteção do S3 para novas contas que ingressam na sua organização.

Console

A conta de GuardDuty administrador delegado pode habilitar novas contas de membros em uma organização por meio do console, usando a página Proteção do S3 ou Contas.

Para habilitar automaticamente a Proteção do S3 para novas contas-membro

1. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.

   Certifique-se de usar as credenciais da conta de GuardDuty administrador delegado.
2. Execute um destes procedimentos:
   - Usando a página Proteção do S3:
     1. No painel de navegação, escolha Proteção do S3.
     2. Na página Proteção do S3, escolha Editar.
     3. Escolha Configurar contas manualmente.
     4. Selecione Habilitar automaticamente para novas contas-membro. Essa etapa garante que sempre que uma nova conta ingressar na sua organização, a Proteção do S3 seja habilitada automaticamente para a conta dessa pessoa. Somente a conta do GuardDuty administrador delegado da organização pode modificar essa configuração.
     5. Escolha Salvar.
   - Como usar a página Contas:
     1. No painel de navegação, selecione Contas.
     2. Na página Contas, escolha Auto-enablepreferências.
     3. Na janela Gerenciar preferências de habilitação automática, selecione Habilitar para novas contas em Proteção do S3.
     4. Escolha Salvar.

API/CLI

- Para ativar seletivamente o S3 Protection para suas contas de membros, invoque a operação da UpdateOrganizationConfigurationAPI usando a sua própria. *`detector ID`*
- O exemplo a seguir mostra como você pode habilitar a Proteção do S3 para uma conta de membro único. Defina as preferências para habilitar ou desabilitar automaticamente o plano de proteção nessa região para novas contas (`NEW`) que ingressam na organização, todas as contas (`ALL`) ou nenhuma das contas (`NONE`) na organização. Para obter mais informações, consulte auto EnableOrganizationMembers. Com base na sua preferência, talvez seja necessário substituir `NEW` por `ALL` ou `NONE`.

  Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no https://console.aws.amazon.com/guardduty/console ou execute a ListDetectorsAPI.

  ```
  aws guardduty update-organization-configuration --detector-
  id 12abc34d567e8fa901bc2d34e56789f0 --auto-enable --features '[{"Name":
   "S3_DATA_EVENTS", "autoEnable": "NEW"}]'
  ```

- Quando o código é executado com êxito, ele retorna uma lista vazia de `UnprocessedAccounts`. Se houver algum problema na alteração das configurações do detector de uma conta, esse ID de conta será listado junto com um resumo do problema.

Habilite seletivamente a Proteção do S3 nas contas-membro

Escolha seu método de acesso preferido para habilitar seletivamente a Proteção do S3 para contas-membro.

Console

1. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.

   Certifique-se de usar as credenciais da conta de GuardDuty administrador delegado.
2. No painel de navegação, selecione Contas.

   Na página Contas, analise a coluna Proteção do S3 para ver o status da sua conta-membro.

3. Para habilitar seletivamente a Proteção do S3

   Selecione a conta para a qual deseja configurar a Proteção do S3. Você pode selecionar várias contas ao mesmo tempo. No menu suspenso Editar planos de proteção, selecione S3Pro e escolha a opção apropriada.

API/CLI

Para habilitar ou desabilitar seletivamente a Proteção do S3 para suas contas-membro, execute a operação da API updateMemberDetectors usando seu próprio ID de detector. O exemplo a seguir mostra como você pode habilitar a Proteção do S3 para uma conta de membro único. Para desabilitá-la, substitua `true` por `false`.

Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no https://console.aws.amazon.com/guardduty/console ou execute a ListDetectorsAPI.

```
 aws guardduty update-member-detectors --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 123456789012 --features
 '[{"Name" : "S3_DATA_EVENTS", "Status" : "ENABLED"}]'
```

> **Note**
>
> Também é possível passar uma lista de IDs de conta separados por um espaço.

Quando o código é executado com êxito, ele retorna uma lista vazia de `UnprocessedAccounts`. Se houver algum problema na alteração das configurações do detector de uma conta, esse ID de conta será listado junto com um resumo do problema.

> **Note**
>
> Se você usa scripts para integrar novas contas e deseja desabilitar a Proteção do S3 em suas novas contas, você pode modificar a operação da API createDetector com o objeto `dataSources` opcional, conforme descrito neste tópico.

Ativando a Proteção do S3 para uma conta independente

Uma conta autônoma é responsável pela decisão de ativar ou desativar um plano de proteção Conta da AWS em uma conta específica Região da AWS.

Se sua conta estiver associada a uma conta de GuardDuty administrador por meio AWS Organizations ou pelo método de convite, esta seção não se aplica à sua conta. Para obter mais informações, consulte Habilitando a Proteção do S3 em ambientes de várias contas.

Depois de ativar o S3 Protection, GuardDuty começará a monitorar AWS CloudTrail os eventos de dados dos buckets do S3 em sua conta.

Selecione seu método de acesso preferido para configurar a Proteção do S3 para uma conta independente.

Console

1. Faça login no Console de gerenciamento da AWS e abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.
2. No seletor de seletor de Região do canto superior direito, selecione a Região a ser habilitada a Proteção do S3.
3. No painel de navegação, escolha Proteção do S3.
4. A página Proteção do S3 fornece o status atual da Proteção do S3 para sua conta. É possível Habilitar ou Desabilitar a Proteção do S3 a qualquer momento.
5. Escolha Confirmar para confirmar sua seleção.

API/CLI

Execute updateDetector usando seu ID de detector válido para a Região atual e passando o `name` do objeto `features` como `S3_DATA_EVENTS` definido para `ENABLED` para habilitar a Proteção do S3, respectivamente.

> **Note**
>
> Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no https://console.aws.amazon.com/guardduty/console ou execute a ListDetectorsAPI.

Como alternativa, você pode usar AWS Command Line Interface. Para ativar o S3 Protection, execute o comando a seguir e *12abc34d567e8fa901bc2d34e56789f0* substitua-o pelo ID do detector da sua conta e *us-east-1* pela região em que você deseja ativar o S3 Protection.

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
region us-east-1 --features '[{"Name" : "S3_DATA_EVENTS", "Status" : "ENABLED"}]'
```

GuardDuty Monitoramento de execução

> **Note**
>
> Você pode configurar o Runtime Monitoring junto com todos os outros planos de proteção em uma única página no GuardDuty console. Para obter mais informações, consulte Configurando planos de proteção.

O Runtime Monitoring observa e analisa eventos em nível de sistema operacional, rede e arquivos para ajudá-lo a detectar possíveis ameaças em cargas de AWS trabalho específicas em seu ambiente.

AWS Recursos compatíveis com o Runtime Monitoring — O Runtime Monitoring fornece cobertura de detecção de ameaças para os recursos do Amazon Elastic Kubernetes Service (Amazon EKS), Amazon Elastic Container Service (Amazon ECS) on e Amazon AWS Fargate Elastic Compute Cloud (Amazon EC2).

GuardDuty não é compatível com clusters do Amazon EKS em execução no AWS Fargate.

Neste documento e em outras seções relacionadas ao Runtime Monitoring, GuardDuty usa a terminologia do tipo de recurso para se referir aos recursos do Amazon EKS, do Fargate, do Amazon ECS e do Amazon EC2.

O Runtime Monitoring usa um agente de GuardDuty segurança que adiciona visibilidade ao comportamento do tempo de execução, como acesso a arquivos, execução de processos, argumentos de linha de comando e conexões de rede. Para cada tipo de recurso que deseja monitorar para possíveis ameaças, pode-se gerenciar o agente de segurança para esse tipo de recurso específico de forma automática ou manual (com exceção do Fargate (somente Amazon ECS)). Gerenciar o agente de segurança automaticamente significa que você permite GuardDuty instalar e atualizar o agente de segurança em seu nome. Por outro lado, ao gerenciar manualmente o agente de segurança de seus recursos, é sua responsabilidade instalar e atualizar o agente de segurança, conforme necessário.

Com esse recurso estendido, GuardDuty pode ajudá-lo a identificar e responder a possíveis ameaças que podem atingir aplicativos e dados em execução em suas cargas de trabalho e instâncias individuais. Por exemplo, uma ameaça pode começar comprometendo um único contêiner que executa uma aplicação Web vulnerável. Essa aplicação Web pode ter permissões de acesso

aos contêineres e workloads subjacentes. Nesse cenário, credenciais configuradas incorretamente podem levar a um acesso mais amplo à conta e aos dados nela armazenados.

Ao analisar os eventos de tempo de execução dos contêineres e cargas de trabalho individuais, é GuardDuty possível identificar o comprometimento de um contêiner e das AWS credenciais associadas em uma fase inicial e detectar tentativas de escalar privilégios, solicitações de API suspeitas e acesso malicioso aos dados em seu ambiente.

Conteúdo

- Como funcionam
- Como funciona o teste gratuito de 30 dias no Monitoramento de runtime
- Pré-requisitos para habilitar o Monitoramento de runtime
- Habilitando o GuardDuty monitoramento de tempo
- Gerenciando agentes GuardDuty de segurança
- Analisando estatísticas de cobertura de runtime e solucionando problemas
- Configurar o monitoramento da CPU e da memória
- Como usar uma VPC compartilhada com Monitoramento de Runtime
- Usando a Infraestrutura como Código (IaC) com agentes de segurança GuardDuty automatizados
- Tipos de eventos de tempo de execução coletados que GuardDuty usam
- Agente de hospedagem de repositórios Amazon ECR GuardDuty
- Dois agentes de segurança no mesmo host subjacente
- Monitoramento de execução do EKS em GuardDuty
- GuardDuty versões de lançamento do agente de segurança
- Desativação, desinstalação e remoção de recursos no Monitoramento de runtime

Como funcionam

O Runtime Monitoring usa um agente de segurança leve para observar o comportamento em tempo de execução de suas cargas de trabalho do Amazon EC2, Amazon EKS e Amazon ECS nas cargas de trabalho do Fargate e detectar ameaças. Funciona de ponta a ponta da seguinte forma:

1. O agente é implantado em seus recursos. GuardDuty pode implantar e atualizar o agente para você (configuração automatizada do agente) ou você mesmo pode implantá-lo e gerenciá-lo (configuração manual do agente). As etapas dependem do tipo de recurso.

2. O agente coleta eventos de tempo de execução. Em cada recurso monitorado, o agente observa a atividade no nível do sistema operacional, como execução de processos, acesso a arquivos e conexões de rede.
3. O agente envia eventos para GuardDuty. O agente entrega os eventos ao GuardDuty back-end. Os dados permanecem na AWS rede e GuardDuty não cobram pelos eventos transmitidos de seus recursos computacionais para o. GuardDuty Para obter detalhes, consulte Como o agente de segurança se conecta ao GuardDuty.
4. GuardDuty analisa os eventos e gera descobertas. Quando detecta um comportamento suspeito, como aumento de privilégios ou comunicação com um host mal-intencionado conhecido, GuardDuty gera uma descoberta. Para ver a lista atualizada das descobertas GuardDuty geradas, consulteGuardDuty Tipos de descoberta de monitoramento de tempo de execução.

O agente é executado dentro dos limites definidos de CPU e memória, portanto, seu consumo de recursos permanece previsível e não prejudica o desempenho ou a disponibilidade das cargas de trabalho executadas no mesmo host. Para esses limites, consultePré-requisitos para habilitar o Monitoramento de runtime.

Conteúdo

- Como habilitar o monitoramento de runtime
- Implantação do agente de segurança no Amazon EKS
- Implantação do agente de segurança no Amazon EC2
- Implantação do agente de segurança no Amazon ECS no Fargate
- Como o agente de segurança se conecta ao GuardDuty
- Rastreando a cobertura do monitoramento do

Como habilitar o monitoramento de runtime

Habilitar o Runtime Monitoring é um processo de duas etapas:

1. Ative o Runtime Monitoring para sua conta. GuardDuty em seguida, aceita eventos de tempo de execução de suas instâncias do Amazon EC2, clusters do Amazon ECS e cargas de trabalho do Amazon EKS.
2. Gerencie o agente de GuardDuty segurança dos recursos que você deseja monitorar. Com base no tipo de recurso, você pode:

- Use a configuração automatizada do agente — GuardDuty implanta o agente e estabelece sua conectividade.
- Gerencie o agente manualmente — você cria um VPC endpoint e gerencia a instalação e as atualizações do agente.

O gerenciamento do agente difere de acordo com o tipo de recurso. Para obter detalhes, consulte:

- Implantação do agente de segurança no Amazon EKS
- Implantação do agente de segurança no Amazon EC2
- Implantação do agente de segurança no Amazon ECS no Fargate

Quando o agente GuardDuty de segurança é implantado em uma instância do Amazon EC2 e recebe eventos de tempo de execução dela GuardDuty , Conta da AWS você não cobra pela análise dos logs de fluxo de VPC dessa instância. Isso evita custos duplos de uso.

Implantação do agente de segurança no Amazon EKS

GuardDuty O Runtime Monitoring monitora ameaças em seus clusters do Amazon EKS implantando o agente GuardDuty de segurança neles. No Amazon EKS, GuardDuty implanta o agente como complemento `aws-guardduty-agent` do EKS.

> **Observações**
>
> O Monitoramento de Runtime é compatível com clusters do Amazon EKS em execução em instâncias do Amazon EC2 e do Amazon EKS Auto Mode.
> O Monitoramento de Runtime não é compatível com clusters do Amazon EKS com Amazon EKS Hybrid Nodes e aqueles em execução no AWS Fargate.
> Para ter mais informações sobre recursos do Amazon EKS, consulte O que é o Amazon EKS? no Guia do usuário do Amazon EKS.

Você pode permitir que você GuardDuty gerencie o agente automaticamente (recomendado) ou gerencie-o manualmente.

Configuração automatizada do agente (recomendada)

GuardDuty gerencia a implantação e as atualizações do agente de segurança para seus clusters EKS. No GuardDuty console, essa configuração aparece como Runtime Monitoring (EKS).

Para saber como o agente de segurança se conecta GuardDuty, consulteComo o agente de segurança se conecta ao GuardDuty.

Impacto da ativação do agente de segurança

GuardDuty implanta o agente de segurança em seus clusters EKS, e o Amazon Elastic Kubernetes Service (Amazon EKS) coordena sua implantação nos nós.

Escopo de monitoramento

Por padrão, GuardDuty gerencia o agente de segurança para todos os clusters EKS em sua conta, incluindo os novos clusters que você cria. Para parar GuardDuty de gerenciar o agente em um cluster específico, adicione a tag`GuardDutyManaged`: `false` a esse cluster.

Para obter mais informações sobre a marcação de clusters do EKS, consulte Como marcar seus recursos do Amazon EKS no Guia do usuário do Amazon EKS.

Considerações

- Quando a configuração automatizada do agente está desativada, GuardDuty gerencia o agente de segurança somente nos clusters EKS com os quais você marca`GuardDutyManaged`:`true`.
- Adicionar a `false` tag`GuardDutyManaged`: GuardDuty impede o gerenciamento do agente de segurança, mas não desinstala um agente que já esteja instalado.
- Proteja a `GuardDutyManaged` tag controlando quem pode modificá-la usando políticas de controle de serviço ou políticas do IAM. Para obter mais informações, consulte Políticas de controle de serviços (SCPs) no Guia do usuário do AWS Organizations ou Controlar o acesso a recursos da AWS no Guia do usuário do IAM.

Configuração manual do agente

Use essa abordagem quando quiser implantar e gerenciar manualmente o agente de GuardDuty segurança em todos os seus clusters EKS. Certifique-se de que o Runtime Monitoring esteja ativado para suas contas. O agente GuardDuty de segurança pode não funcionar conforme o esperado se o Runtime Monitoring não estiver ativado.

Impacto do uso dessa abordagem

Você deve coordenar a implantação do agente de GuardDuty segurança em seus clusters EKS em todas as suas contas. Para obter os recursos de segurança mais recentes, você também deve atualizar o agente ao GuardDuty lançar uma nova versão. Para obter mais informações sobre versões do agente no EKS, consulte GuardDuty versões do agente de segurança para recursos do Amazon EKS.

Considerações

Você deve oferecer suporte ao fluxo de dados seguro enquanto monitora e aborda as lacunas de cobertura à medida que novos clusters e workloads são implantados continuamente.

Tópicos relacionados

- Como o agente de segurança se conecta ao GuardDuty
- Rastreando a cobertura do monitoramento do

Implantação do agente de segurança no Amazon EC2

GuardDuty O Runtime Monitoring monitora ameaças em suas instâncias do Amazon EC2 implantando o agente de GuardDuty segurança nelas.

> **Note**
>
> O Runtime Monitoring também coleta eventos de tempo de execução de tarefas do Amazon ECS executadas em suas instâncias do Amazon EC2.

Você pode permitir que você GuardDuty gerencie o agente automaticamente (recomendado) ou gerencie-o manualmente.

Configuração automatizada do agente (recomendada)

GuardDuty gerencia a implantação e as atualizações do agente de segurança para suas instâncias do Amazon EC2. No GuardDuty console, essa configuração aparece como Runtime Monitoring (EC2).

Para saber como o agente de segurança se conecta GuardDuty, consulteComo o agente de segurança se conecta ao GuardDuty.

Impacto da ativação do agente de segurança

Com a configuração automatizada do agente, GuardDuty cria uma associação SSM para suas instâncias do SSM-managed Amazon EC2 (mostrada no Fleet Manager https://console.aws.amazon.com/systems-manager/no console) e a usa para instalar e atualizar o agente.

Escopo de monitoramento

Por padrão, GuardDuty gerencia o agente de segurança para todas as instâncias do Amazon EC2 em sua conta. Para parar GuardDuty de gerenciar o agente em uma instância específica, adicione a tag`GuardDutyManaged`: `false` a essa instância.

Considerações

- Quando a configuração automática do agente está desativada, GuardDuty gerencia o agente de segurança somente nas instâncias do Amazon EC2 que você identifica com`GuardDutyManaged`:. `true`
- Adicionar a `false` tag`GuardDutyManaged`: GuardDuty impede o gerenciamento do agente de segurança, mas não desinstala um agente que já esteja instalado.
- Proteja a `GuardDutyManaged` tag controlando quem pode modificá-la usando políticas de controle de serviço ou políticas do IAM. Para obter mais informações, consulte Políticas de controle de serviços (SCPs) no Guia do usuário do AWS Organizations ou Controlar o acesso a recursos da AWS no Guia do usuário do IAM.

Configuração manual do agente

Há duas maneiras de gerenciar manualmente o agente de segurança do Amazon EC2:

- Para instâncias do SSM-managed Amazon EC2, você pode usar documentos GuardDuty gerenciados AWS Systems Manager para instalar o agente de segurança.

> **Note**
>
> Para usar essa opção, certifique-se de que cada nova instância do Amazon EC2 que você iniciar esteja habilitada para SSM.

- Use scripts do gerenciador de pacotes RPM (RPM) para instalar o agente de segurança em suas instâncias do Amazon EC2, sejam elas gerenciadas por SSM ou não.

Tópicos relacionados

- Como o agente de segurança se conecta ao GuardDuty
- Rastreando a cobertura do monitoramento do

Implantação do agente de segurança no Amazon ECS no Fargate

GuardDuty O Runtime Monitoring monitora ameaças em seus clusters do Amazon ECS no Fargate, implantando GuardDuty o agente de segurança neles.

> **Note**
>
> O Monitoramento de Runtime não oferece suporte a aplicações executadas em instâncias gerenciadas do Amazon ECS.

GuardDuty gerencia o agente automaticamente; o gerenciamento manual não está disponível para o Fargate. No GuardDuty console, essa configuração aparece como Runtime Monitoring (ECS).

Configuração automatizada do agente (recomendada)

GuardDuty gerencia a implantação e as atualizações do agente de segurança para novas tarefas do Fargate em seus clusters do Amazon ECS.

Para saber como o agente de segurança se conecta GuardDuty, consulteComo o agente de segurança se conecta ao GuardDuty.

Impacto da ativação do agente de segurança

Para cada nova tarefa do Fargate, GuardDuty anexa um contêiner auxiliar que executa o agente de segurança e coleta os eventos de tempo de execução dos contêineres na tarefa.

A imagem auxiliar é armazenada no Amazon Elastic Container Registry (Amazon ECR), com camadas no Amazon S3, e é extraída quando a tarefa é iniciada. Dependendo da configuração da rede, talvez seja necessário permitir o acesso ao ECR e ao S3. Por exemplo, permita a lista de prefixos gerenciados do S3 se você usar grupos de segurança restritos. Para obter mais informações, consulte Pré-requisitos para acesso à imagem do contêiner.

Se o sidecar não puder ser iniciado, o Runtime Monitoring não impedirá a execução da tarefa. As tarefas do Fargate não podem ser modificadas depois de iniciadas, então GuardDuty conecta o sidecar na inicialização da tarefa.

Escopo de monitoramento

Por padrão, GuardDuty gerencia o agente de segurança para todos os clusters do Amazon ECS em sua conta. Para parar GuardDuty de gerenciar o agente em um cluster específico, adicione a tag`GuardDutyManaged`: `false` a esse cluster.

Para obter mais informações sobre como gerenciar o agente para tarefas do Fargate, consulte. Gerenciamento de agente de segurança automatizado para Fargate (somente Amazon ECS)

Considerações

- Quando a configuração automatizada do agente está desativada, GuardDuty gerencia o agente de segurança somente nos clusters do Amazon ECS com os quais você marca`GuardDutyManaged`:`true`.
- Adicionar a `false` tag`GuardDutyManaged`: GuardDuty impede o gerenciamento do agente de segurança, mas não desinstala um agente que já esteja instalado.
- Proteja a `GuardDutyManaged` tag controlando quem pode modificá-la usando políticas de controle de serviço ou políticas do IAM. Para obter mais informações, consulte Políticas de controle de serviços (SCPs) no Guia do usuário do AWS Organizations ou Controlar o acesso a recursos da AWS no Guia do usuário do IAM.

Tópicos relacionados

- Como o agente de segurança se conecta ao GuardDuty
- Rastreando a cobertura do monitoramento do

Como o agente de segurança se conecta ao GuardDuty

O agente de segurança Runtime Monitoring fornece eventos de tempo de execução para GuardDuty. Os dados permanecem na AWS rede. Não há custo adicional para a conectividade que GuardDuty configura. Para autenticar o agente, GuardDuty use os papéis de identidade da instância. Para o Amazon ECS no Fargate GuardDuty , usa a função de execução de tarefas; consulte. Requisitos de permissão

GuardDuty suporta dois métodos de conectividade: link-local e Amazon VPC endpoint. O agente de segurança tenta se conectar usando esses métodos para entregar eventos de tempo de execução ao GuardDuty.

Com a configuração automatizada do agente, GuardDuty estabelece a conectividade automaticamente. Se você gerenciar o agente manualmente, precisará criar um endpoint da Amazon VPC.

Link-local conectividade

O agente se conecta ao GuardDuty back-end por meio de um endereço local de link, em. `guardduty-data-v2.us-east-1.amazonaws.com` Link-locala conectividade não usa DNS privado. O Região da AWS (*us-east-1*) muda com base na sua região.

Conectividade de endpoint Amazon VPC

O agente se conecta ao GuardDuty back-end por meio de um endpoint da Amazon VPC. Ele resolve e se conecta ao nome DNS privado do endpoint. Para um endpoint não FIPS, isso é. `guardduty-data.us-east-1.amazonaws.com` O Região da AWS (*us-east-1*) muda com base na sua região.

O recurso deve ter um caminho de rede válido para um endpoint ativo `guardduty-data` da Amazon VPC. GuardDuty seleciona a sub-rede com base na disponibilidade de IP, portanto, para topologias de rede avançadas, valide se a conectividade é possível.

Pré-requisitos

Para conhecer os pré-requisitos, consulte Pré-requisitos para habilitar o Monitoramento de runtime.

Considerações

- Todas as VPCs — Com a configuração automatizada de agentes, GuardDuty configura a conectividade em todas as suas VPCs, incluindo VPCs centralizadas e faladas. Para obter mais informações sobre VPCs centralizadas, consulte Interface de VPC endpoints no AWS Whitepaper - Construindo uma infraestrutura de rede escalável e segura. Multi-VPC AWS
- VPC compartilhada — Se você usa uma VPC compartilhada, usa GuardDuty essa VPC compartilhada para receber eventos de tempo de execução de seus recursos depois que os pré-requisitos forem atendidos. Consulte Como usar uma VPC compartilhada com Monitoramento de Runtime.

Tópicos relacionados

- Implantação do agente de segurança no Amazon EC2
- Implantação do agente de segurança no Amazon EKS
- Implantação do agente de segurança no Amazon ECS no Fargate
- Analisando estatísticas de cobertura de runtime e solucionando problemas

Rastreando a cobertura do monitoramento do

Depois de habilitar o Runtime Monitoring e instalar o agente de GuardDuty segurança em sua conta independente ou em várias contas de membros, você pode seguir as etapas a seguir para garantir que a configuração do plano de proteção esteja funcionando conforme o esperado e monitorar a quantidade de memória e CPU que o agente de GuardDuty segurança usa.

Avalie a cobertura de runtime

GuardDuty recomenda que você avalie continuamente o status da cobertura do recurso em que você implantou o agente de segurança. O status da cobertura pode ser Íntegro ou Não íntegro. Um status de cobertura íntegra indica que GuardDuty está recebendo os eventos de tempo de execução do recurso correspondente quando há uma atividade no nível do sistema operacional.

Quando o status da cobertura se torna íntegro para o recurso, GuardDuty é capaz de receber os eventos de tempo de execução e analisá-los para detecção de ameaças. Quando GuardDuty detecta uma possível ameaça à segurança nas tarefas ou aplicativos em execução nas cargas de trabalho e instâncias do seu contêiner, GuardDuty gera. GuardDuty Tipos de descoberta de monitoramento de tempo de execução

Você também pode configurar um Amazon EventBridge (EventBridge) para receber uma notificação quando o status da cobertura mudar de Insalubre para Saudável ou de outra forma. Para obter mais informações, consulte Analisando estatísticas de cobertura de runtime e solucionando problemas.

Configurar o monitoramento de CPU e memória para o agente GuardDuty de segurança

Depois de avaliar se o status da cobertura é exibido como Íntegro, você pode avaliar o desempenho do agente de segurança para seu tipo de recurso. Para clusters do Amazon EKS que têm o agente de segurança versão v1.5 ou superior, GuardDuty suporta a configuração dos parâmetros do agente de segurança (complementar). Para obter mais informações, consulte Configurar o monitoramento da CPU e da memória.

Como funciona o teste gratuito de 30 dias no Monitoramento de runtime

O período de teste gratuito de 30 dias funciona de forma diferente para as novas GuardDuty contas e as contas existentes que já habilitaram o EKS Runtime Monitoring antes de a capacidade de Runtime Monitoring ser estendida às instâncias do Amazon EC2 e AWS Fargate (somente Amazon ECS).

Estou usando o período de GuardDuty teste ou nunca habilitei o EKS Runtime Monitoring

A lista a seguir explica como o período de teste gratuito de 30 dias funciona se você estiver usando o período de teste de GuardDuty 30 dias ou nunca tiver ativado o EKS Runtime Monitoring:

- Quando você ativa GuardDuty pela primeira vez, o Runtime Monitoring e o EKS Runtime Monitoring não serão ativados por padrão.

  Ao ativar o Runtime Monitoring para sua conta ou organização, certifique-se também de configurar o agente de GuardDuty segurança para o recurso que você deseja monitorar para detecção de ameaças. Por exemplo, se quiser usar o Monitoramento de runtime para suas instâncias do Amazon EC2, depois de habilitar o Monitoramento de runtime, você também deverá configurar o agente de segurança para o Amazon EC2. Você pode optar por fazer isso manualmente ou automaticamente por meio de GuardDuty.
- O plano de proteção de Monitoramento de runtime está ativado no nível da conta. O período de avaliação gratuita de 30 dias funciona no nível do recurso. Depois que o agente GuardDuty de segurança é implantado em um tipo de recurso específico, o teste gratuito de 30 dias começa quando GuardDuty recebe seu primeiro evento de tempo de execução associado a esse tipo de recurso. Por exemplo, você implantou o GuardDuty agente no nível do recurso (para a instância do Amazon EC2, o cluster do Amazon ECS e o cluster do Amazon EKS). Quando GuardDuty receber o primeiro evento de tempo de execução de uma instância do Amazon EC2, o teste gratuito de 30 dias começará somente para o Amazon EC2.
- Quando você deseja ativar somente o EKS Runtime Monitoring — Quando você ativa GuardDuty pela primeira vez, o EKS Runtime Monitoring não é ativado por padrão (após o lançamento do Runtime Monitoring). É preciso habilitar o Monitoramento de runtime do EKS. Para usá-lo de forma ideal, certifique-se de gerenciar o agente de GuardDuty segurança manualmente ou ativar a configuração automática do agente para que ele GuardDuty gerencie o agente em seu nome.

Seu período de teste gratuito de 30 dias do EKS Runtime Monitoring começa quando GuardDuty recebe seu primeiro evento de tempo de execução para o recurso Amazon EKS.

Eu habilitei o Monitoramento de runtime do EKS antes do lançamento do Monitoramento de runtime

Use esta seção somente quando o EKS Runtime Monitoring estiver ativado para você Conta da AWS e agora você quiser migrar para o Runtime Monitoring.

A lista a seguir inclui cenários que podem se aplicar ao seu caso de uso para habilitar o Monitoramento de runtime:

- Para uma GuardDuty conta existente que tem o plano de proteção do EKS Runtime Monitoring ativado e usa a experiência do GuardDuty console para usar esse plano de proteção, com o anúncio do Runtime Monitoring, a experiência do console do EKS Runtime Monitoring agora foi consolidada no Runtime Monitoring. Sua configuração existente para o Monitoramento de runtime EKS permanece a mesma. Você pode continuar usando o API/CLI suporte para realizar operações associadas ao EKS Runtime Monitoring.
- Para usar o Monitoramento de runtime do EKS como parte do Monitoramento de runtime, você precisará configurar o Monitoramento de runtime para sua conta ou organização. Para manter a mesma configuração para o Monitoramento de runtime, consulte Migração do Monitoramento de runtime do EKS para o Monitoramento de runtime. No entanto, isso não afetará sua avaliação gratuita de 30 dias do recurso Amazon EKS.
- O plano de proteção de Monitoramento de runtime está ativado no nível da conta por Região. Depois que o agente de GuardDuty segurança é implantado em um dos tipos de recursos especificados (instância do Amazon EC2 e cluster do Amazon ECS), o teste gratuito de 30 dias começa GuardDuty quando recebe o primeiro evento de tempo de execução associado ao recurso. Para cada tipo de recurso há uma avaliação gratuita de 30 dias.

  Por exemplo, depois de ativar o Runtime Monitoring, você opta por implantar o GuardDuty agente somente na instância do Amazon EC2. O teste gratuito de 30 dias desse recurso começará somente quando GuardDuty receber seu primeiro evento de tempo de execução para uma instância do Amazon EC2. Posteriormente, quando você implantar o GuardDuty agente para o Fargate (somente Amazon ECS), o teste gratuito de 30 dias desse recurso começará somente quando GuardDuty receber seu primeiro evento de tempo de execução para o cluster Amazon ECS. Considerando que você já tem o EKS Runtime Monitoring ativado para sua conta, GuardDuty não redefine o teste gratuito de 30 dias de um recurso do Amazon EKS.

Pré-requisitos para habilitar o Monitoramento de runtime

Para habilitar o Runtime Monitoring e gerenciar o agente de GuardDuty segurança, você deve atender aos pré-requisitos de cada tipo de recurso que deseja monitorar para detecção de ameaças. Cada tipo de recurso tem pré-requisitos diferentes. Por exemplo, GuardDuty oferece suporte a diferentes distribuições de sistema operacional com base no tipo de recurso.

Caso queira monitorar apenas os recursos do Amazon EC2, é necessário seguir os pré-requisitos das instâncias do Amazon EC2.. Caso opte por monitorar os recursos do Amazon EKS posteriormente, é preciso seguir os pré-requisitos específicos dos clusters do Amazon EKS.

As seções a seguir incluem pré-requisitos com base no tipo de recurso.

Conteúdo

- Pré-requisitos para suporte de instância do Amazon EC2
- Pré-requisitos para o suporte do Bottlerocket ECS-EC2
- Pré-requisitos para AWS Fargate Suporte (somente para Amazon ECS)
- Pré-requisitos para o suporte ao cluster do Amazon EKS
- Arquiteturas de CPU, sistemas operacionais e versões do kernel compatíveis

Pré-requisitos para suporte de instância do Amazon EC2

Esta seção inclui os pré-requisitos para monitorar o comportamento de runtime das instâncias do Amazon EC2. Depois que esses pré-requisitos forem atendidos, consulte Habilitando o GuardDuty monitoramento de tempo.

Tópicos

- Tornar as instâncias do EC2 gerenciadas por SSM (somente para configuração automatizada de agentes)
- Validação dos requisitos de arquitetura
- Validando a política de controle de serviço da sua organização em um ambiente de várias contas
- Ao usar a configuração de agente automatizado
- Limite de CPU e memória para o GuardDuty agente
- Próxima etapa

Tornar as instâncias do EC2 gerenciadas por SSM (somente para configuração automatizada de agentes)

GuardDuty usa AWS Systems Manager (SSM) para implantar, instalar e gerenciar automaticamente o agente de segurança em suas instâncias. Se você planeja instalar e gerenciar manualmente o GuardDuty agente, o SSM não é necessário.

Para gerenciar suas instâncias do Amazon EC2 com o Systems Manager, consulte Configurando o Systems Manager para instâncias do Amazon EC2 no Guia do usuário do AWS Systems Manager .

Validação dos requisitos de arquitetura

A arquitetura da distribuição do sistema operacional pode afetar o comportamento do agente de GuardDuty segurança. Você deve atender aos seguintes requisitos para usar o Monitoramento de runtime para instâncias do Amazon EC2:

Para obter as arquiteturas de CPU, as distribuições do sistema operacional e as versões do kernel verificadas, consulte. Arquiteturas de CPU, sistemas operacionais e versões do kernel compatíveis

- Requisitos adicionais - Somente se você tiver o Amazon ECS/Amazon EC2

  Para o Amazon ECS/Amazon EC2, recomendamos que você use as ECS-optimized AMIs mais recentes da Amazon (datadas de 29 de setembro de 2023 ou posterior) ou use a versão v1.77.0 do agente do Amazon ECS.

Visualizando e atualizando valores **`RLIMIT_MEMLOCK`**

Quando o `RLIMIT_MEMLOCK` limite do seu sistema é definido como muito baixo, o agente de GuardDuty segurança pode não funcionar conforme projetado. GuardDuty recomenda que os limites rígidos e flexíveis sejam de pelo menos 32 MB. Se você não atualizar os limites, não GuardDuty conseguirá monitorar os eventos de tempo de execução do seu recurso. Quando `RLIMIT_MEMLOCK` está acima dos limites mínimos estabelecidos, torna-se opcional que você atualize esses limites.

Você pode modificar o `RLIMIT_MEMLOCK` valor padrão antes ou depois de instalar o agente GuardDuty de segurança.

Para visualizar valores de **`RLIMIT_MEMLOCK`**

1. Executar `ps aux | grep guardduty`. Isso exibirá o ID do processo (`pid`).
2. Copie o ID do processo (`pid`) da saída do comando anterior.

3. Execute `grep "Max locked memory" /proc/pid/limits` após substituir o `pid` pelo ID do processo copiado da etapa anterior.

   Isso exibirá a memória máxima bloqueada para executar o agente GuardDuty de segurança.

Para atualizar os valores do **`RLIMIT_MEMLOCK`**

1. Se o arquivo `/etc/systemd/system.conf.d/NUMBER-limits.conf` existir, comente a linha de `DefaultLimitMEMLOCK` desse arquivo. Esse arquivo define um `RLIMIT_MEMLOCK` padrão com alta prioridade, que substitui suas configurações no arquivo `/etc/systemd/system.conf`.
2. Abra o arquivo `/etc/systemd/system.conf` e remova o comentário da linha com `#DefaultLimitMEMLOCK=`.
3. Atualize o valor padrão fornecendo limites de `RLIMIT_MEMLOCK` rígidos e flexíveis de pelo menos 32 MB. A atualização deve ter a seguinte aparência: `DefaultLimitMEMLOCK=32M:32M`. O formato é `soft-limit:hard-limit`.
4. Executar `sudo reboot`.

Validando a política de controle de serviço da sua organização em um ambiente de várias contas

Se você configurou uma política de controle de serviços (SCP) para gerenciar permissões em sua organização, valide se o limite de permissões permite a ação. `guardduty:SendSecurityTelemetry` GuardDuty requer essa permissão para oferecer suporte ao Runtime Monitoring em diferentes tipos de recursos.

Se sua conta for uma conta de membro, entre em contato com o administrador delegado associado. Para obter informações sobre o gerenciamento de SCPs para a sua organização, consulte Política de controle de serviços (SCPs).

Ao usar a configuração de agente automatizado

Para Configuração automatizada do agente (recomendada) isso, você Conta da AWS deve atender aos seguintes pré-requisitos:

- Ao usar tags de inclusão com configuração automática de agentes, GuardDuty para criar uma associação SSM para uma nova instância, certifique-se de que a nova instância seja

gerenciada por SSM e apareça no Fleet Manager no https://console.aws.amazon.com/systems-manager/console.

- Ao usar tags de exclusão com configuração de agente automatizado:
  - Adicione a `false` tag`GuardDutyManaged`: antes de configurar o agente GuardDuty automatizado para sua conta.

    Certifique-se de adicionar a tag de exclusão às instâncias do Amazon EC2 antes de iniciá-las. Depois de habilitar a configuração automatizada do agente para o Amazon EC2, qualquer instância do EC2 que seja executada sem uma tag de exclusão será coberta GuardDuty pela configuração automática do agente.
  - Habilite a configuração Permitir tags nos metadados para suas instâncias. Essa configuração é necessária porque é GuardDuty necessário ler a tag de exclusão do serviço de metadados da instância (IMDS) para determinar se ela deve excluir a instância da instalação do agente. Para obter mais informações, consulte Habilitar o acesso a tags em metadados da instância no Guia do usuário do Amazon EC2.

Limite de CPU e memória para o GuardDuty agente

Limite da CPU

GuardDuty limita o agente de segurança a 10% da capacidade total da vCPU na instância. Por exemplo, em uma instância com 4 núcleos de vCPU, o agente pode usar no máximo 0,4 vCPU.

Limite de memória

Da memória associada à sua instância do Amazon EC2, há uma memória limitada que o agente de GuardDuty segurança pode usar.

A tabela a seguir mostra o limite de memória.

Memória da instância do Amazon EC2.	Memória máxima para GuardDuty agente
Menor que 8 GB	128 MB
8 GB a menos de 32 GB	256 MB
Maior que ou igual a 32 GB	1 GB

Próxima etapa

A próxima etapa é configurar o Monitoramento de runtime e também gerenciar o agente de segurança (automática ou manualmente).

Pré-requisitos para o suporte do Bottlerocket ECS-EC2

> **Important**
>
> Esta seção se aplica somente à versão de ECS-optimized AMIs do Bottlerocket `v1.62.1` e superior, incluindo as seguintes variantes:
>
> - `bottlerocket-aws-ecs-2-x86_64` / `bottlerocket-aws-ecs-2-aarch64`
> - `bottlerocket-aws-ecs-3-x86_64` / `bottlerocket-aws-ecs-3-aarch64`
> - `bottlerocket-aws-ecs-2-nvidia` / `bottlerocket-aws-ecs-2-nvidia-fips`
> - `bottlerocket-aws-ecs-3-nvidia` / `bottlerocket-aws-ecs-3-nvidia-fips`

GuardDutyO Runtime Monitoring estende a detecção de ameaças às suas instâncias do Amazon EC2 da Bottlerocket nos clusters do Amazon ECS, usando um agente de segurança que funciona como um contêiner hospedeiro para se adequar ao design otimizado de contêineres da Bottlerocket. Para habilitá-lo, preencha os pré-requisitos desta seção. Depois que esses pré-requisitos forem atendidos, consulte Habilitando o GuardDuty monitoramento de tempo.

Para obter mais informações sobre requisitos e instruções, consulteGerenciando o agente GuardDuty de segurança no Bottlerocket (Amazon ECS no Amazon EC2).

Tópicos

- Faça com que as instâncias do EC2 sejam gerenciadas por SSM e configure as permissões da instância
- Validação dos requisitos de arquitetura
- Requisitos de conectividade de rede
- Validando a política de controle de serviço da sua organização em um ambiente de várias contas
- Ao usar a configuração de agente automatizado
- Limite de CPU e memória para o GuardDuty agente
- Próxima etapa

Faça com que as instâncias do EC2 sejam gerenciadas por SSM e configure as permissões da instância

GuardDuty usa AWS Systems Manager (SSM) para implantar, instalar e gerenciar o agente de segurança em suas instâncias do Bottlerocket, executando o agente SSM no contêiner de controle do Bottlerocket.

Na maioria dos casos, as permissões que suas instâncias já têm para o Bottlerocket também abrangem. GuardDuty Nenhuma política adicional é necessária. A `AmazonEC2ContainerRegistryReadOnly` política que a Bottlerocket usa para extrair suas imagens de contêiner de controle e administração também atende aos requisitos GuardDuty da Bottlerocket de extrair a imagem do contêiner do agente. Para obter mais informações, consulte o README do Bottlerocket.

O perfil da instância deve incluir as seguintes políticas gerenciadas:

- `AmazonSSMManagedInstanceCore`— Necessário para que o contêiner de controle Bottlerocket execute o agente SSM. Para gerenciar suas instâncias do Amazon EC2 com o Systems Manager, consulte Configurando o Systems Manager para instâncias do Amazon EC2 no Guia do usuário do AWS Systems Manager .
- `AmazonEC2ContainerRegistryReadOnly`— Necessário para extrair a imagem do contêiner do GuardDuty agente do Amazon ECR. No mínimo, as seguintes permissões são necessárias:

```
...
      "ecr:GetAuthorizationToken",
      "ecr:BatchCheckLayerAvailability",
      "ecr:GetDownloadUrlForLayer",
      "ecr:BatchGetImage",
...
```

Para restringir ainda mais as permissões do Amazon ECR, você pode adicionar o URI do repositório do Amazon ECR que hospeda o agente de GuardDuty segurança do Amazon ECS-Amazon EC2 Bottlerocket. Para obter mais informações, consulte Repositório ECR para GuardDuty agente em Bottlerocket ECS-EC2.

Validação dos requisitos de arquitetura

A arquitetura de suas instâncias determina como o agente GuardDuty de segurança se comporta. O Bottlerocket ECS-2 e suas ECS-3 variantes atendem a esses requisitos prontos para uso. Confirme o seguinte antes de ativar o Runtime Monitoring:

- O suporte do kernel inclui `eBPFTracepoints`, e. `Kprobe` As variantes do Bottlerocket usam kernel `6.1` e ECS-3 as ECS-2 variantes usam kernel. `6.12` Ambas as versões atendem aos requisitos do kernel para o Runtime Monitoring. A opção `CONFIG_DEBUG_INFO_BTF=y` kernel está habilitada por padrão em ECS-2 Bottlerocket e kernels. ECS-3
- Para arquiteturas de CPU, o Runtime Monitoring é compatível com AMD64 (`x86_64`) e ARM64 (). `aarch64`

Requisitos de conectividade de rede

GuardDuty hospeda seu agente de segurança como uma imagem de contêiner no Amazon ECR, então suas instâncias precisam de conectividade de rede com o Amazon ECR para extraí-lo. Dependendo da configuração da rede, escolha uma das seguintes opções:

Opção 1 – usar o acesso à rede pública (se disponível)

Se suas instâncias do Bottlerocket forem executadas em sub-redes com acesso de saída à Internet, nenhuma configuração de rede adicional será necessária.

Opção 2 – usar endpoints da Amazon VPC (para sub-redes privadas)

Para instâncias do Bottlerocket em sub-redes privadas, os VPC endpoints fornecem a conectividade de que o agente precisa. Configure endpoints para Amazon ECR, Amazon S3 e Systems Manager para que as instâncias possam extrair a imagem do agente e se comunicar com o Systems Manager para implantação.

Para obter mais informações sobre a configuração de VPC endpoints, consulte Criar os VPC endpoints para o Amazon ECR no Amazon Elastic Container Registry User Guide e Create VPC endpoints no User Guide.AWS Systems Manager

Validando a política de controle de serviço da sua organização em um ambiente de várias contas

Se você configurou uma política de controle de serviços (SCP) para gerenciar permissões em sua organização, valide se o limite de permissões permite a ação. `guardduty:SendSecurityTelemetry` GuardDuty requer essa permissão para oferecer suporte ao Runtime Monitoring em diferentes tipos de recursos.

Se sua conta for uma conta de membro, entre em contato com o administrador delegado associado. Para obter informações sobre o gerenciamento de SCPs para a sua organização, consulte Política de controle de serviços (SCPs).

Ao usar a configuração de agente automatizado

Para usar a configuração automatizada do agente, você Conta da AWS deve atender aos seguintes pré-requisitos:

- Ao usar tags de inclusão com configuração automática de agentes, GuardDuty para criar uma associação SSM para uma nova instância, certifique-se de que a nova instância seja gerenciada por SSM e apareça no Fleet Manager no https://console.aws.amazon.com/systems-manager/console.
- Ao usar tags de exclusão com configuração de agente automatizado:
  - Adicione a `false` tag`GuardDutyManaged`: a uma instância do Amazon EC2 antes de iniciá-la e antes de configurar o agente GuardDuty automatizado para sua conta. Depois que a configuração automatizada do agente é ativada, qualquer instância iniciada sem uma tag de exclusão é coberta automaticamente.
  - Habilite a configuração Permitir tags nos metadados para suas instâncias. Essa configuração é necessária porque é GuardDuty necessário ler a tag de exclusão do serviço de metadados da instância (IMDS) para determinar se ela deve excluir a instância da instalação do agente. Para obter mais informações, consulte Habilitar o acesso a tags em metadados da instância no Guia do usuário do Amazon EC2.

Limite de CPU e memória para o GuardDuty agente

Limite da CPU

GuardDuty limita o agente de segurança a 10% da capacidade total da vCPU na instância. Por exemplo, em uma instância com 4 núcleos de vCPU, o agente pode usar no máximo 0,4 vCPU.

Limite de memória

Da memória associada à sua instância do Amazon EC2, há um limite na memória que o agente de GuardDuty segurança pode usar.

A tabela a seguir mostra o limite de memória.

Memória da instância do Amazon EC2.	Memória máxima para GuardDuty agente
Menor que 8 GB	128 MB
8 GB a menos de 32 GB	256 MB
Maior que ou igual a 32 GB	1 GB

Próxima etapa

Sua próxima etapa é configurar o Runtime Monitoring e gerenciar o agente de segurança automaticamente.

Pré-requisitos para AWS Fargate Suporte (somente para Amazon ECS)

Esta seção inclui os pré-requisitos para monitorar o comportamento em tempo de execução de seus Fargate-Amazon recursos do ECS. Depois que esses pré-requisitos forem atendidos, consulte Habilitando o GuardDuty monitoramento de tempo.

Tópicos

- Validação dos requisitos de arquitetura
- Pré-requisitos para acesso à imagem do contêiner
- Validando a política de controle de serviço da sua organização em um ambiente de várias contas
- Validação de permissões de perfis e limite de permissões de política
- Limites de CPU e memória

Validação dos requisitos de arquitetura

A plataforma que você usa pode afetar o suporte do agente GuardDuty de segurança GuardDuty no recebimento de eventos de tempo de execução de seus clusters do Amazon ECS. Você precisa validar que está usando uma das plataformas verificadas.

Considerações iniciais:

A AWS Fargate plataforma para seus clusters do Amazon ECS deve ser Linux. A versão da plataforma correspondente deve ser pelo menos`1.4.0` ou`LATEST`. Para obter mais informações sobre as versões de plataforma, consulte Versões da plataforma Linux no Guia do desenvolvedor do Amazon Elastic Container Service.

As versões da plataforma Windows ainda não são suportadas.

Para obter as arquiteturas de CPU, as distribuições do sistema operacional e as versões do kernel verificadas, consulte. Arquiteturas de CPU, sistemas operacionais e versões do kernel compatíveis

Pré-requisitos para acesso à imagem do contêiner

Os pré-requisitos a seguir ajudam você a acessar a imagem do contêiner auxiliar GuardDuty a partir do repositório Amazon ECR.

Requisitos de permissão

A função de execução da tarefa exige determinadas permissões do Amazon Elastic Container Registry (Amazon ECR) para baixar a imagem do contêiner GuardDuty do agente de segurança:

```
...
      "ecr:GetAuthorizationToken",
      "ecr:BatchCheckLayerAvailability",
      "ecr:GetDownloadUrlForLayer",
      "ecr:BatchGetImage",
...
```

Para restringir ainda mais as permissões do Amazon ECR, você pode adicionar o URI do repositório do Amazon ECR que hospeda o agente de GuardDuty segurança para (somente AWS Fargate Amazon ECS). Para obter mais informações, consulte Agente de hospedagem de repositórios Amazon ECR GuardDuty.

Você pode usar a política AmazonECSTaskExecutionRolePolicygerenciada ou adicionar as permissões acima à sua `TaskExecutionRole` política.

Configuração de definição de tarefas

Ao criar ou atualizar os serviços do Amazon ECS, você precisa fornecer informações de sub-rede na definição da sua tarefa:

A execução das UpdateServiceAPIs CreateServicee na Referência de API do Amazon Elastic Container Service exige que você passe as informações da sub-rede. Para obter mais informações, consulte Definições da tarefa do Amazon ECS no Guia do desenvolvedor do Amazon Elastic Container Service.

Requisitos de conectividade de rede

Você deve garantir a conectividade de rede para baixar a imagem do GuardDuty contêiner do Amazon ECR. Esse requisito é específico GuardDuty porque ele usa o Amazon ECR para hospedar seu agente de segurança. Dependendo da configuração da sua rede, você deve implementar uma das seguintes opções:

Opção 1 – usar o acesso à rede pública (se disponível)

Se suas tarefas do Fargate forem executadas em sub-redes com acesso de saída à Internet, nenhuma configuração de rede adicional será necessária.

Opção 2 – usar endpoints da Amazon VPC (para sub-redes privadas)

Se suas tarefas do Fargate forem executadas em sub-redes privadas sem acesso à Internet, você deverá configurar VPC endpoints para ECR para garantir que o URI do repositório ECR que hospeda o agente de segurança esteja acessível pela rede. GuardDuty Sem esses endpoints, as tarefas em sub-redes privadas não podem baixar a imagem do GuardDuty contêiner.

Para obter instruções de configuração do endpoint da VPC, consulte Criação dos endpoints da VPC para o Amazon ECR no Guia do usuário do Amazon Elastic Container Registry.

Para obter informações sobre como permitir que o Fargate baixe o GuardDuty contêiner, consulte Como usar imagens do Amazon ECR com o Amazon ECS no Guia do usuário do Amazon Elastic Container Registry.

Configuração do security group

As imagens do GuardDuty contêiner estão no Amazon ECR e exigem acesso ao Amazon S3. Esse requisito é específico para baixar imagens de contêiner do Amazon ECR. Para tarefas com acesso restrito à rede, você deve configurar seus grupos de segurança para permitir acesso ao S3.

Adicione uma regra de saída em seu grupo de segurança que permita o tráfego para a lista de prefixos gerenciados do S3 (`pl-xxxxxxxx`) na porta 443. Para obter uma regra de saída, consulte Configurar regras de grupo de segurança no Guia do usuário da Amazon VPC.

Para visualizar suas listas AWS de prefixos gerenciados no console ou descrevê-las usando AWS Command Line Interface (AWS CLI), consulte listas de prefixos AWS gerenciados no Guia do usuário da Amazon VPC.

Validando a política de controle de serviço da sua organização em um ambiente de várias contas

Esta seção explica como validar suas configurações de política de controle de serviços (SCP) para garantir que o Monitoramento de Runtime funcione conforme esperado na sua organização.

Se você configurou uma ou mais políticas de controle de serviços para gerenciar permissões na sua organização, você deve confirmar se ela não nega a ação `guardduty:SendSecurityTelemetry`. Para obter informações sobre como os SCPs funcionam, consulte Avaliação do SCP no Guia do usuário do AWS Organizations .

Se sua conta for uma conta de membro, entre em contato com o administrador delegado associado. Para obter informações sobre o gerenciamento de SCPs para a sua organização, consulte Políticas de controle de serviços (SCPs) noGuia do usuário das AWS Organizations .

Execute as etapas a seguir para todos os SCPs que você configurou em seu ambiente de várias contas:

Para validar o **`dever de proteção: não SendSecurityTelemetry é negado`** no SCP

1. Faça login no console Organizations em https://console.aws.amazon.com/organizations/. Você deve fazer login como um perfil do IAM ou como o usuário-raiz (não recomendado) na conta gerencial da organização.
2. No painel de navegação à esquerda, selecione Policies (Políticas). Em seguida, em Tipos de políticas compatíveis, selecione Políticas de controle de serviços.
3. Na página Políticas de controle de serviços, escolha o nome da política que deseja validar.
4. Na página de detalhes da política, veja o Conteúdo dessa política. Confirme que ele não nega a ação `guardduty:SendSecurityTelemetry`.

   A política de SCP a seguir é um exemplo para não negar a ação `guardduty:SendSecurityTelemetry`:

   JSON

```
{
```

```
    "Version":"2012-10-17",
    "Statement": [
        {
    "Effect": "Allow",
            "Action": [
                "guardduty:SendSecurityTelemetry"
            ],
            "Resource": "*"
        }
    ]
}
```

Se sua política negar essa ação, você deverá atualizar a política. Para obter mais informações, consulte Atualização de uma política de controle de serviços (SCP) no Guia do usuário do AWS Organizations .

Validação de permissões de perfis e limite de permissões de política

Use as etapas a seguir para validar se os limites de permissões associados à função e sua política não restringem a `guardduty:SendSecurityTelemetry` ação.

Para visualizar o limite de permissões para perfis e sua política

1. Faça login no Console de gerenciamento da AWS e abra o console do IAM em https://console.aws.amazon.com/iam/.
2. No painel de navegação esquerdo, em Gerenciamento de acesso, escolha Perfis.
3. Na página Perfis, selecione o perfil *`TaskExecutionRole`* que você pode ter criado.
4. Na página do perfil selecionado, na guia Permissões, expanda o nome da política associada a esse perfil. Em seguida, confirme se essa política não restringe `guardduty:SendSecurityTelemetry`.
5. Se o limite de permissões estiver definido, expanda essa seção. Em seguida, expanda cada política para verificar se ela não restringe a ação `guardduty:SendSecurityTelemetry`. A política deve ter a seguinte aparência: Example SCP policy.

   Conforme necessário, execute uma das seguintes ações:

- Para modificar a política, selecione Editar. Na página Modificar permissões dessa política, atualize a política no Editor de políticas. Confirme se o esquema JSON permanece válido. Em seguida, escolha Próximo. Em seguida, você poderá revisar e salvar as alterações.
- Para alterar esse limite de permissões e escolher outro limite, escolha Alterar limite.
- Para remover esse limite de permissões, escolha Remover limite.

Para obter informações sobre como gerenciar políticas, consulte Políticas e permissões no AWS Identity and Access Management no Guia do usuário do IAM.

Limites de CPU e memória

Na definição de tarefa Fargate, você deve especificar o valor de CPU e de memória no nível de tarefa. A tabela a seguir mostra as combinações válidas de valores de CPU e memória em nível de tarefa e o limite máximo de memória do agente de GuardDuty segurança correspondente para o GuardDuty contêiner.

Valor de CPU	Valor de memória	GuardDuty limite máximo de memória do agente
256 (0,25 vCPU)	512 MiB, 1 GB, 2GB	128 MB
512 (0,5 vCPU)	1 GB, 2 GB, 3 GB, 4 GB	
1024 (1 vCPU)	2 GB, 3 GB, 4 GB	
	5 GB, 6 GB, 7 GB, 8 GB	
2048 (2 vCPU)	Entre 4 GB e 16 GB em incrementos de 1 GB	
4096 (4 vCPU)	Entre 8 GB e 20 GB em incrementos de 1 GB	
8192 (8 vCPU)	Entre 16 GB e 28 GB em incrementos de 4 GB	256 MB

Valor de CPU	Valor de memória	GuardDuty limite máximo de memória do agente
	Entre 32 GB e 60 GB em incrementos de 4 GB	512 MB
16384 (16 vCPU)	Entre 32 GB e 120 GB em incrementos de 8 GB	1 GB

Depois de habilitar o Monitoramento de runtime e avaliar se o status da cobertura do seu cluster é Íntegro, você pode configurar e visualizar as métricas do Container insight. Para obter mais informações, consulte Como configurar o monitoramento no cluster do Amazon ECS.

A próxima etapa é configurar o Monitoramento de runtime e também configurar o agente de segurança.

Pré-requisitos para o suporte ao cluster do Amazon EKS

Esta seção inclui os pré-requisitos para monitorar o comportamento de runtime de seus recursos do Amazon EKS. Esses pré-requisitos são cruciais para que o GuardDuty agente funcione conforme o esperado. Depois que esses pré-requisitos forem atendidos, consulte Habilitando o GuardDuty monitoramento de tempo para começar a monitorar seus recursos.

Suporte para recursos do Amazon EKS

O monitoramento de runtime é compatível com clusters do Amazon EKS em execução em instâncias do Amazon EC2 e do Amazon EKS Auto Mode.

O Monitoramento de Runtime não é compatível com clusters do Amazon EKS com Amazon EKS Hybrid Nodes e aqueles em execução no AWS Fargate.

Para ter mais informações sobre recursos do Amazon EKS, consulte O que é o Amazon EKS? no Guia do usuário do Amazon EKS.

Validação dos requisitos de arquitetura

A plataforma que você usa pode afetar a forma como o GuardDuty Security Agent oferece suporte GuardDuty ao recebimento de eventos de tempo de execução de seus clusters EKS. Você precisa

validar que está usando uma das plataformas verificadas. Se você estiver gerenciando o GuardDuty agente manualmente, certifique-se de que a versão do Kubernetes seja compatível com a versão do GuardDuty agente que está em uso no momento.

Plataformas verificadas

Para obter as arquiteturas de CPU, as distribuições do sistema operacional e as versões do kernel verificadas, consulte. Arquiteturas de CPU, sistemas operacionais e versões do kernel compatíveis

Atualmente, com a versão do kernel `5.4` em ARM64 (`aarch64`), não é GuardDuty possível gerar GuardDuty Tipos de descoberta de monitoramento de tempo de execução que estejam relacionados a. Eventos do Sistema de Nomes de Domínio (DNS)

Versões do Kubernetes suportadas pelo agente de segurança GuardDuty

A tabela a seguir mostra as versões do Kubernetes para seus clusters EKS que são compatíveis com o agente de GuardDuty segurança.

Versão complementar do agente de GuardDuty segurança Amazon EKS	Versão do Kubernetes
v1.17.1 (mais recente - v1.17.1-eksbuild.2)	1,31 - 1,36
v1.16.0 (mais recente - v1.16.0-eksbuild.2)	1,28 - 1,36
v1.15.0 (mais recente - v1.15.0-eksbuild.2)	1,28 - 1,36
v1.12.2 (mais recente - v1.12.2-eksbuild.2)	1,28 - 1,36
v1.12.1 (mais recente - v1.12.1-eksbuild.4)	1,28 - 1,35
v1.11.0 (mais recente - v1.11.0-eksbuild.4)	1,28 - 1,34
v1.10.0 (mais recente – v1.10.0-eksbuild.2)	1,21 - 1,33
v1.9.0 (mais recente – v1.9.0-eksbuild.2) v1.8.1 (mais recente – v1.8.1-eksbuild.2)	1,21 - 1,32
v1.7.1 v1.7.0	1,21 - 1,31

Versão complementar do agente de GuardDuty segurança Amazon EKS	Versão do Kubernetes
v1.6.1	
v1.6.0 v1.5.0 v1.4.1 v1.4.0 v1.3.1	1,21 - 1,29
v1.3.0 v1.2.0	1,21 - 1,28
v1.1.0	1,21 - 1,26
v1.0.0	1.21 - 1.25

Algumas das versões do agente de GuardDuty segurança chegarão ao fim do suporte padrão.

Para obter informações sobre as versões de lançamento do agente, consulte GuardDuty versões do agente de segurança para recursos do Amazon EKS.

Limites de CPU e memória

A tabela a seguir mostra os limites de CPU e memória do complemento Amazon EKS para GuardDuty (`aws-guardduty-agent`).

Parâmetro	Limite mínimo	Limite máximo
CPU	200 m	1000 m
Memória	256 Mi	1024 Mi

Quando você usa a versão 1.5.0 ou superior do complemento Amazon EKS, GuardDuty fornece a capacidade de configurar o esquema complementar para seus valores de CPU e memória. Para obter informações sobre o intervalo de configuração, consulte Parâmetros e valores configuráveis.

Depois de ativar o Monitoramento de runtime do EKS e avaliar o status de cobertura dos seus clusters do EKS, você pode configurar e visualizar as métricas de insights do contêiner. Para obter mais informações, consulte Configurar o monitoramento da CPU e da memória.

Validando sua política de controle de serviço da organização

Se você configurou uma política de controle de serviços (SCP) para gerenciar permissões em sua organização, verifique se o limite de permissões não é restritivo. `guardduty:SendSecurityTelemetry` GuardDuty requer essa permissão para oferecer suporte ao Runtime Monitoring em diferentes tipos de recursos.

Se sua conta for uma conta de membro, entre em contato com o administrador delegado associado. Para obter informações sobre o gerenciamento de SCPs para a sua organização, consulte Política de controle de serviços (SCPs).

Arquiteturas de CPU, sistemas operacionais e versões do kernel compatíveis

Esta seção consolida as arquiteturas de CPU, as distribuições do sistema operacional e as versões do kernel que foram verificadas para oferecer suporte ao agente de segurança. GuardDuty A menos que um tipo de recurso seja chamado separadamente, esses requisitos se aplicam ao Runtime Monitoring para instâncias do Amazon EC2 (somente AWS Fargate Amazon ECS) e clusters do Amazon EKS.

O suporte do kernel inclui `eBPFTracepoints`, e. `Kprobe` Para arquiteturas de CPU, o monitoramento de runtime é compatível com AMD64 (`x64`) e ARM64 (Graviton2 e superior)[1].

A tabela a seguir mostra as distribuições do sistema operacional e as versões do kernel que foram verificadas para oferecer suporte ao agente GuardDuty de segurança.

Distribuição do sistema operacional [2]	Versão do kernel [3]
Amazon Linux 2	5.4[4], 5.10[4], 5.15

Distribuição do sistema operacional [2]	Versão do kernel [3]
Amazon Linux 2023	5.4[4], 5.10[4], 5.15, 6.1, 6.5, 6.8, 6.12
Ubuntu 20.04, 22.04, 24.04, 26.04	5,4 [4], 5,10, 5,15 [4], 6,5, 6,8, 6,13, 6,14, 6,15, 6,16, 6,17, 6,18, 7,0
Debian 11, 12, 13	5.4[4], 5.10[4], 5.15, 6.1, 6.5, 6.8, 6.12
RedHat 9,4, 10,2	5.14, 6.12
Fedora 34, 40, 41, 43, 44	5,11, 5,17, 6,8, 6,12, 7,1
CentOS Stream 9, 10	5.14, 6.12
Oracle Linux 8.9, 9.3	5.15
Rocky Linux 9.5, 10.1	5.14, 6.12
Alma Linux 9, 10	5.14, 6.12
Servidor SUSE Linux Enterprise 16	6.12
Foguete de garrafas	5,4 [4], 5,10, 5,15 [4], 6,1, 6,18

1. O Runtime Monitoring não oferece suporte à instância Graviton de primeira geração, como os tipos de instância A1.
2. Suporte para vários sistemas operacionais - GuardDuty verificou o suporte do Runtime Monitoring para a distribuição operacional listada na tabela anterior. Embora o agente GuardDuty de segurança possa ser executado em sistemas operacionais não listados na tabela anterior, a GuardDuty equipe não pode garantir o valor de segurança esperado.
3.

Para qualquer versão do kernel, você deve definir o sinalizador `CONFIG_DEBUG_INFO_BTF` como y (isto é, verdadeiro). Isso é necessário para que o agente GuardDuty de segurança possa ser executado conforme o esperado.

Para AWS Fargate (somente Amazon ECS), essa opção de kernel é gerenciada pelo Fargate e não requer nenhuma ação de sua parte.

4. Para as versões 5.10 e anteriores do kernel, o agente GuardDuty de segurança usa memória bloqueada na RAM (`RLIMIT_MEMLOCK`) para funcionar conforme o esperado. Se o `RLIMIT_MEMLOCK` valor do seu sistema estiver definido como muito baixo, GuardDuty recomenda definir limites rígidos e flexíveis para pelo menos 32 MB. Para obter informações sobre como verificar e modificar o `RLIMIT_MEMLOCK` valor padrão nas instâncias do Amazon EC2, consulte. Visualizando e atualizando valores `RLIMIT_MEMLOCK`

Habilitando o GuardDuty monitoramento de tempo

Antes de ativar o Monitoramento de runtime em sua conta, certifique-se de que o tipo de recurso para o qual você deseja monitorar os eventos de runtime suporte os requisitos da plataforma. Para obter mais informações, consulte Pré-requisitos.

Se você usa o Monitoramento de runtime do EKS antes do lançamento do Monitoramento de runtime, pode usar as APIs para verificar e atualizar a configuração existente do Monitoramento de runtime do EKS. Você também pode migrar sua configuração existente do Monitoramento de runtime do EKS para o Monitoramento de runtime. Para obter mais informações, consulte Migração do Monitoramento de runtime do EKS para o Monitoramento de runtime.

> **Note**
>
> Atualmente, esta documentação fornece etapas para habilitar o Monitoramento de runtime para suas contas e organização somente por console. Você também pode ativar o Runtime Monitoring usando ações de API ou AWS CLI for GuardDuty.

Você pode configurar o Monitoramento de runtime usando as etapas nos tópicos a seguir.

Conteúdo

- Habilitando o Monitoramento de runtime do EKS para ambientes com várias contas

- Habilitando o Monitoramento de runtime para uma conta autônoma

Habilitando o Monitoramento de runtime do EKS para ambientes com várias contas

Em ambientes com várias contas, somente a conta de GuardDuty administrador delegado pode ativar ou desativar o Runtime Monitoring para as contas dos membros e gerenciar a configuração automatizada do agente para os tipos de recursos pertencentes às contas dos membros em sua organização. As contas GuardDuty dos membros não podem modificar essa configuração em suas contas. A conta de GuardDuty administrador delegado gerencia suas contas de membros usando AWS Organizations. Para obter mais informações sobre ambientes com várias contas, consulte Gerenciar de várias contas.

Para conta de GuardDuty administrador delegado

Para habilitar o Runtime Monitoring para uma conta de GuardDuty administrador delegado

1. Faça login no Console de gerenciamento da AWS e abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.
2. No painel de navegação, escolha Monitoramento de runtime.
3. Na guia Configuração, escolha Editar na seção Configuração do Monitoramento de runtime.
4. Como usar a opção Habilitar para todas as contas

   Se você quiser ativar o Runtime Monitoring para todas as contas que pertencem à organização, incluindo a conta de GuardDuty administrador delegado, escolha Habilitar para todas as contas.
5. Como usar a opção Configurar contas manualmente

   Se você quiser habilitar o Monitoramento de runtime para cada conta-membro individualmente, escolha Configurar contas manualmente.

   - Selecione Habilitar na seção Administrador delegado (esta conta).
6. Gerencie o agente de segurança para seu tipo de recurso. Para obter mais informações, consulte Gerenciando agentes GuardDuty de segurança.

Para todas as contas-membro

Para habilitar o Monitoramento de runtime para todas as contas-membro na organização

1. Faça login no Console de gerenciamento da AWS e abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.

   Faça login usando a conta de GuardDuty administrador delegado.
2. No painel de navegação, escolha Monitoramento de runtime.
3. Na página Monitoramento de runtime, na guia Configuração, escolha Editar na seção Configuração do Monitoramento de runtime.
4. Escolha Habilitar para todas as contas.
5. Gerencie o agente de segurança para seu tipo de recurso. Para obter mais informações, consulte Gerenciando agentes GuardDuty de segurança.

Para todas as contas-membro ativas existentes

Para habilitar o Monitoramento de runtime para contas-membro existentes na organização

1. Faça login no Console de gerenciamento da AWS e abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.

   Faça login usando a conta de GuardDuty administrador delegado da organização.
2. No painel de navegação, escolha Monitoramento de runtime.
3. Na página Monitoramento de runtime, na guia Configuração, é possível ver o status atual da configuração do Monitoramento de runtime.
4. No painel Monitoramento de runtime, na seção Contas-membro ativas, escolha Ações.
5. No menu suspenso Ações, escolha Habilitar para todas as contas-membro ativas existentes.
6. Escolha Confirmar.
7. Gerencie o agente de segurança para seu tipo de recurso. Para obter mais informações, consulte Gerenciando agentes GuardDuty de segurança.

> **Note**
>
> Pode levar até 24 horas para atualizar a configuração das contas-membro.

Auto-enable Monitoramento de tempo de execução somente para contas de novos membros

Para habilitar o Monitoramento de runtime para novas contas-membro na organização

1. Faça login no Console de gerenciamento da AWS e abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.

   Faça login usando a conta de GuardDuty administrador delegado designada da organização.
2. No painel de navegação, escolha Monitoramento de runtime
3. Na guia Configuração, escolha Editar na seção Configuração do Monitoramento de runtime.
4. Escolha Configurar contas manualmente.
5. Selecione Habilitar automaticamente para novas contas-membro.
6. Gerencie o agente de segurança para seu tipo de recurso. Para obter mais informações, consulte Gerenciando agentes GuardDuty de segurança.

Somente para contas-membro ativas seletivas

Para habilitar o Monitoramento de runtime para contas-membro individuais ativas

1. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.

   Faça login usando as credenciais da conta de GuardDuty administrador delegado.
2. No painel de navegação, selecione Contas.
3. Na página Contas, revise os valores nas colunas Monitoramento de runtime e Gerenciar o agente automaticamente. Esses valores indicam se o Runtime Monitoring e o gerenciamento de GuardDuty agentes estão habilitados ou não habilitados para a conta correspondente.
4. Na tabela Contas, selecione a conta para a qual você deseja habilitar o Monitoramento de runtime. É possível escolher várias contas ao mesmo tempo.
5. Escolha Confirmar.
6. Selecione Editar planos de proteção. Escolha a ação apropriada.
7. Escolha Confirmar.
8. Gerencie o agente de segurança para seu tipo de recurso. Para obter mais informações, consulte Gerenciando agentes GuardDuty de segurança.

Habilitando o Monitoramento de runtime para uma conta autônoma

Uma conta autônoma é responsável pela decisão de ativar ou desativar um plano de proteção Conta da AWS em uma conta específica Região da AWS.

Se sua conta estiver associada a uma conta de GuardDuty administrador por meio AWS Organizations ou pelo método de convite, esta seção não se aplica à sua conta. Para obter mais informações, consulte Habilitando o Monitoramento de runtime do EKS para ambientes com várias contas.

Depois de ativar o Runtime Monitoring, certifique-se de instalar o agente GuardDuty de segurança por meio de configuração automatizada ou implantação manual. Como parte da conclusão de todas as etapas listadas no procedimento a seguir, certifique-se de instalar o agente de segurança.

Para habilitar o Monitoramento de runtime em conta autônoma

1. Faça login no Console de gerenciamento da AWS e abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.
2. No painel de navegação, escolha Monitoramento de runtime.
3. Na guia Configuração, escolha Habilitar para ativar o Monitoramento de runtime para sua conta.
4. Gerencie o agente de segurança para seu tipo de recurso. Para obter mais informações, consulte Gerenciando agentes GuardDuty de segurança.

Gerenciando agentes GuardDuty de segurança

Você pode gerenciar o agente de GuardDuty segurança do recurso que deseja monitorar. Se você quiser monitorar mais de um tipo de recurso, certifique-se de gerenciar o GuardDuty agente desse recurso.

Os tópicos a seguir ajudarão você nas próximas etapas para gerenciar o agente de segurança.

Conteúdo

- Habilitando o agente de segurança automatizado para a instância do Amazon EC2
- Gerenciando o agente de segurança manualmente para o recurso do Amazon EC2
- Gerenciando o agente GuardDuty de segurança no Bottlerocket (Amazon ECS no Amazon EC2)
- Gerenciamento de agente de segurança automatizado para Fargate (somente Amazon ECS)

- Gerenciando automaticamente o agente de segurança para recursos do Amazon EKS
- Como gerenciar o agente de segurança manualmente para o cluster Amazon EKS
- Configurar parâmetros do agente de GuardDuty segurança (complemento) para o Amazon EKS
- Validando a configuração do endpoint da VPC

Habilitando o agente de segurança automatizado para a instância do Amazon EC2

Esta seção inclui etapas para habilitar o agente GuardDuty automatizado para seus recursos do Amazon EC2 em sua conta independente ou em um ambiente de várias contas.

Antes de continuar, verifique se todas Pré-requisitos para suporte de instância do Amazon EC2 foram seguidas.

Tópicos

- GuardDuty Agente habilitador para recursos do Amazon EC2 em ambiente de várias contas
- Habilitando um agente GuardDuty automatizado para recursos do Amazon EC2 em uma conta independente
- Migração do agente manual do Amazon EC2 para o agente automatizado

Se você estiver migrando do gerenciamento manual do GuardDuty agente para a ativação do agente GuardDuty automatizado, antes de seguir as etapas para habilitar o agente GuardDuty automatizado, consulteMigração do agente manual do Amazon EC2 para o agente automatizado.

GuardDuty Agente habilitador para recursos do Amazon EC2 em ambiente de várias contas

Em ambientes com várias contas, somente a conta de GuardDuty administrador delegado pode ativar ou desativar a configuração automática do agente para os tipos de recursos pertencentes às contas membros em sua organização. As contas GuardDuty dos membros não podem modificar essa configuração em suas contas. A conta de GuardDuty administrador delegado gerencia suas contas de membros usando AWS Organizations. Para obter mais informações sobre ambientes com várias contas, consulte Gerenciar de várias contas.

Para conta de GuardDuty administrador delegado

Configure for all instances

Se você escolher Habilitar para todas as contas do Runtime Monitoring, escolha uma das seguintes opções para a conta de GuardDuty administrador delegado:

- Opção 1

  Em Configuração de agente automatizado, na seção EC2, selecione Habilitar para todas as contas.

- Opção 2
  - Em Configuração de agente automatizado, na seção EC2, selecione Configurar contas manualmente.
  - Selecione Habilitar em Administrador delegado (esta conta).
- Escolha Salvar.

Se você escolheu Configurar contas manualmente na seção Monitoramento de runtime, execute as seguintes etapas:

- Em Configuração de agente automatizado, na seção EC2, selecione Configurar contas manualmente.
- Selecione Habilitar em Administrador delegado (esta conta).
- Escolha Salvar.

Independentemente da opção escolhida para habilitar a configuração automatizada do agente para a conta de GuardDuty administrador delegado, você pode verificar se a associação SSM GuardDuty criada instalará e gerenciará o agente de segurança em todos os recursos do EC2 pertencentes a essa conta.

1. Abra o AWS Systems Manager console em https://console.aws.amazon.com/systems-manager/.
2. Abra a guia Destinos da associação SSM (`GuardDutyRuntimeMonitoring-do-not-delete`). Observe que a chave Tag aparece como InstanceIds.

Using inclusion tag in selected instances

Para configurar o GuardDuty agente para instâncias selecionadas do Amazon EC2

1. Faça login no Console de gerenciamento da AWS e abra o console do Amazon EC2 em. https://console.aws.amazon.com/ec2/
2. Adicione a `true` tag`GuardDutyManaged`: às instâncias que você GuardDuty deseja monitorar e detectar possíveis ameaças. Para obter informações sobre como adicionar essa tag, consulte Para adicionar uma tag a um recurso individual.

   Adicionar essa tag permitirá GuardDuty instalar e gerenciar o agente de segurança para essas instâncias EC2 selecionadas. Você não precisa habilitar explicitamente a configuração de agente automatizado.
3. Você pode verificar se a associação SSM GuardDuty criada instalará e gerenciará o agente de segurança somente nos recursos do EC2 que estão marcados com as tags de inclusão.

   Abra o AWS Systems Manager console em https://console.aws.amazon.com/systems-manager/.

   - Abra a guia Destinos da associação SSM que é criada (`GuardDutyRuntimeMonitoring-do-not-delete`). A chave Tag aparece como tag: GuardDutyManaged.

Using exclusion tag in selected instances

> **Note**
>
> Certifique-se de adicionar a tag de exclusão às instâncias do Amazon EC2 antes de iniciá-las. Depois de habilitar a configuração automatizada do agente para o Amazon EC2, qualquer instância do EC2 que seja executada sem uma tag de exclusão será coberta GuardDuty pela configuração automática do agente.

Para configurar o GuardDuty agente para instâncias selecionadas do Amazon EC2

1. Faça login no Console de gerenciamento da AWS e abra o console do Amazon EC2 em. https://console.aws.amazon.com/ec2/

2. Adicione a `false` tag`GuardDutyManaged`: às instâncias que você não GuardDuty deseja monitorar e detectar possíveis ameaças. Para obter informações sobre como adicionar essa tag, consulte Para adicionar uma tag a um recurso individual.
3. Para o etiquetas de exclusão a serem disponibilizadas nos metadados da instância, execute as seguintes etapas:

   a. Na guia Detalhes da sua instância, veja o status de Permitir tags nos metadados da instância.

      Se estiver Desativado no momento, use as etapas a seguir para alterar o status para Ativado. Caso contrário, ignore essa etapa.

   b. No menu Ações, escolha Configurações da instância.

   c. Escolha Permitir tags em metadados de instância.
4. Depois de adicionar a tag de exclusão, execute as mesmas etapas especificadas na guia Configurar para todas as instâncias.

Agora você pode avaliar o runtime Cobertura de runtime e solução de problemas para instância do Amazon EC2.

Auto-enable para todas as contas de membros

> **Note**
>
> Pode levar até 24 horas para atualizar a configuração das contas-membro.

Configure for all instances

As etapas a seguir pressupõem que você escolha Ativar para todas as contas na seção Monitoramento de runtime:

1. Escolha Ativar para todas as contas na seção Configuração automatizada do agente para Amazon EC2.
2. Você pode verificar se a associação SSM que GuardDuty cria (`GuardDutyRuntimeMonitoring-do-not-delete`) instalará e gerenciará o agente de segurança em todos os recursos do EC2 pertencentes a essa conta.

a. Abra o AWS Systems Manager console em https://console.aws.amazon.com/systems-manager/.

b. Abra a guia Destinos para a associação SSM. Observe que a chave Tag aparece como InstanceIds.

Using inclusion tag in selected instances

Para configurar o GuardDuty agente para instâncias selecionadas do Amazon EC2

1. Faça login no Console de gerenciamento da AWS e abra o console do Amazon EC2 em. https://console.aws.amazon.com/ec2/
2. Adicione a `true` tag`GuardDutyManaged`: às instâncias do EC2 que você GuardDuty deseja monitorar e detectar possíveis ameaças. Para obter informações sobre como adicionar essa tag, consulte Para adicionar uma tag a um recurso individual.

   Adicionar essa tag permitirá GuardDuty instalar e gerenciar o agente de segurança para essas instâncias EC2 selecionadas. Você não precisa habilitar explicitamente a configuração de agente automatizado.
3. Você pode verificar se a associação SSM GuardDuty criada instalará e gerenciará o agente de segurança em todos os recursos do EC2 pertencentes à sua conta.

   a. Abra o AWS Systems Manager console em https://console.aws.amazon.com/systems-manager/.

   b. Abra a guia Destinos da associação SSM (`GuardDutyRuntimeMonitoring-do-not-delete`). Observe que a chave Tag aparece como InstanceIds.

Using exclusion tag in selected instances

> **Note**
>
> Certifique-se de adicionar a tag de exclusão às instâncias do Amazon EC2 antes de iniciá-las. Depois de habilitar a configuração automatizada do agente para o Amazon EC2, qualquer instância do EC2 que seja executada sem uma tag de exclusão será coberta GuardDuty pela configuração automática do agente.

Para configurar o agente GuardDuty de segurança para instâncias selecionadas do Amazon EC2

1. Faça login no Console de gerenciamento da AWS e abra o console do Amazon EC2 em. https://console.aws.amazon.com/ec2/
2. Adicione a `false` tag`GuardDutyManaged`: às instâncias que você não GuardDuty deseja monitorar e detectar possíveis ameaças. Para obter informações sobre como adicionar essa tag, consulte Para adicionar uma tag a um recurso individual.
3. Para o etiquetas de exclusão a serem disponibilizadas nos metadados da instância, execute as seguintes etapas:

   a. Na guia Detalhes da sua instância, veja o status de Permitir tags nos metadados da instância.

      Se estiver Desativado no momento, use as etapas a seguir para alterar o status para Ativado. Caso contrário, ignore essa etapa.

   b. No menu Ações, escolha Configurações da instância.

   c. Escolha Permitir tags em metadados de instância.
4. Depois de adicionar a tag de exclusão, execute as mesmas etapas especificadas na guia Configurar para todas as instâncias.

Agora você pode avaliar o runtime Cobertura de runtime e solução de problemas para instância do Amazon EC2.

Auto-enable somente para contas de novos membros

A conta de GuardDuty administrador delegado pode definir a configuração automática do agente para o recurso Amazon EC2 para habilitar automaticamente as novas contas membros à medida que elas ingressam na organização.

Configure for all instances

As etapas a seguir pressupõem que você selecionou Habilitar automaticamente para novas contas-membro na seção Monitoramento de runtime:

1. No painel de navegação, escolha Monitoramento de runtime.
2. Na página Monitoramento de runtime, escolha Editar.
3. Selecione Habilitar automaticamente para novas contas-membro. Essa etapa garante que sempre que uma nova conta ingressar na sua organização, a configuração de agente

automatizado para o Amazon EC2 seja habilitada automaticamente para a conta dessa pessoa. Somente a conta de GuardDuty administrador delegado da organização pode modificar essa seleção.

4. Escolha Salvar.

Quando uma nova conta-membro ingressar na organização, essa configuração será ativada automaticamente para eles. GuardDuty Para gerenciar o agente de segurança das instâncias do Amazon EC2 que pertencem a essa nova conta membro, certifique-se de que todos os pré-requisitos Para uma instância do EC2 sejam atendidos.

Quando uma associação SSM é criada (`GuardDutyRuntimeMonitoring-do-not-delete`), você pode verificar se a associação de SSM instalará e gerenciará o agente de segurança em todas as instâncias do EC2 pertencentes à nova conta-membro.

- Abra o AWS Systems Manager console em https://console.aws.amazon.com/systems-manager/.
- Abra a guia Destinos para a associação SSM. Observe que a chave Tag aparece como InstanceIds.

Using inclusion tag in selected instances

Para configurar o agente GuardDuty de segurança para instâncias selecionadas em sua conta

1. Faça login no Console de gerenciamento da AWS e abra o console do Amazon EC2 em. https://console.aws.amazon.com/ec2/
2. Adicione a `true` tag`GuardDutyManaged`: às instâncias que você GuardDuty deseja monitorar e detectar possíveis ameaças. Para obter informações sobre como adicionar essa tag, consulte Para adicionar uma tag a um recurso individual.

   Adicionar essa tag permitirá GuardDuty instalar e gerenciar o agente de segurança para essas instâncias selecionadas. Você não precisa habilitar explicitamente a configuração de agente automatizado.
3. Você pode verificar se a associação SSM GuardDuty criada instalará e gerenciará o agente de segurança somente nos recursos do EC2 que estão marcados com as tags de inclusão.

   a. Abra o AWS Systems Manager console em https://console.aws.amazon.com/systems-manager/.

b. Abra a guia Destinos para a associação SSM que é criada. A chave Tag aparece como tag: GuardDutyManaged.

Using exclusion tag in selected instances

> **Note**
>
> Certifique-se de adicionar a tag de exclusão às instâncias do Amazon EC2 antes de iniciá-las. Depois de habilitar a configuração automatizada do agente para o Amazon EC2, qualquer instância do EC2 que seja executada sem uma tag de exclusão será coberta GuardDuty pela configuração automática do agente.

Para configurar o agente GuardDuty de segurança para instâncias específicas em sua conta independente

1. Faça login no Console de gerenciamento da AWS e abra o console do Amazon EC2 em. https://console.aws.amazon.com/ec2/
2. Adicione a `false` tag`GuardDutyManaged`: às instâncias que você não GuardDuty deseja monitorar e detectar possíveis ameaças. Para obter informações sobre como adicionar essa tag, consulte Para adicionar uma tag a um recurso individual.
3. Para o etiquetas de exclusão a serem disponibilizadas nos metadados da instância, execute as seguintes etapas:

   a. Na guia Detalhes da sua instância, veja o status de Permitir tags nos metadados da instância.

      Se estiver Desativado no momento, use as etapas a seguir para alterar o status para Ativado. Caso contrário, ignore essa etapa.

   b. No menu Ações, escolha Configurações da instância.

   c. Escolha Permitir tags em metadados de instância.
4. Depois de adicionar a tag de exclusão, execute as mesmas etapas especificadas na guia Configurar para todas as instâncias.

Agora você pode avaliar o runtime Cobertura de runtime e solução de problemas para instância do Amazon EC2.

Somente contas-membro seletivas

Configure for all instances

1. Na página Contas, selecione uma ou mais contas para as quais você deseja habilitar a configuração do Monitoring-Automated agente Runtime (Amazon EC2). Certifique-se de que as contas selecionadas nesta etapa já tenham o Monitoramento de runtime habilitado.
2. Em Editar planos de proteção, escolha a opção apropriada para ativar a configuração do Monitoring-Automated agente Runtime (Amazon EC2).
3. Escolha Confirmar.

Using inclusion tag in selected instances

Para configurar o agente GuardDuty de segurança para instâncias selecionadas

1. Faça login no Console de gerenciamento da AWS e abra o console do Amazon EC2 em. https://console.aws.amazon.com/ec2/
2. Adicione a `true` tag`GuardDutyManaged`: às instâncias que você GuardDuty deseja monitorar e detectar possíveis ameaças. Para obter informações sobre como adicionar essa tag, consulte Para adicionar uma tag a um recurso individual.

   Adicionar essa tag permitirá GuardDuty gerenciar o agente de segurança para suas instâncias marcadas do Amazon EC2. Você não precisa habilitar explicitamente a configuração de agente automatizado (Monitoramento de runtime - Configuração de agente automatizado (EC2).

Using exclusion tag in selected instances

> **Note**
>
> Certifique-se de adicionar a tag de exclusão às instâncias do Amazon EC2 antes de iniciá-las. Depois de habilitar a configuração automatizada do agente para o Amazon EC2, qualquer instância do EC2 que seja executada sem uma tag de exclusão será coberta GuardDuty pela configuração automática do agente.

Para configurar o agente GuardDuty de segurança para instâncias selecionadas

1. Faça login no Console de gerenciamento da AWS e abra o console do Amazon EC2 em. https://console.aws.amazon.com/ec2/
2. Adicione a `false` tag`GuardDutyManaged`: às instâncias do EC2 que você não GuardDuty deseja monitorar ou detectar possíveis ameaças. Para obter informações sobre como adicionar essa tag, consulte Para adicionar uma tag a um recurso individual.
3. Para o etiquetas de exclusão a serem disponibilizadas nos metadados da instância, execute as seguintes etapas:

   a. Na guia Detalhes da sua instância, veja o status de Permitir tags nos metadados da instância.

      Se estiver Desativado no momento, use as etapas a seguir para alterar o status para Ativado. Caso contrário, ignore essa etapa.

   b. No menu Ações, escolha Configurações da instância.

   c. Escolha Permitir tags em metadados de instância.
4. Depois de adicionar a tag de exclusão, execute as mesmas etapas especificadas na guia Configurar para todas as instâncias.

Agora você pode avaliar Cobertura de runtime e solução de problemas para instância do Amazon EC2.

Habilitando um agente GuardDuty automatizado para recursos do Amazon EC2 em uma conta independente

Uma conta autônoma é responsável pela decisão de ativar ou desativar um plano de proteção Conta da AWS em uma conta específica Região da AWS.

Se sua conta estiver associada a uma conta de GuardDuty administrador por meio AWS Organizations ou pelo método de convite, esta seção não se aplica à sua conta. Para obter mais informações, consulte Habilitando o Monitoramento de runtime do EKS para ambientes com várias contas.

Depois de ativar o Runtime Monitoring, certifique-se de instalar o agente GuardDuty de segurança por meio de configuração automatizada ou implantação manual. Como parte da conclusão de todas as etapas listadas no procedimento a seguir, certifique-se de instalar o agente de segurança.

Com base em sua prioridade de monitorar todos os recursos do Amazon EC2 ou recursos seletivos, escolha um método de acordo com sua preferência e siga as etapas da tabela a seguir.

Configure for all instances

Para configurar o Monitoramento de runtime para todas as instâncias em sua conta autônoma

1. Faça login no Console de gerenciamento da AWS e abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.
2. No painel de navegação, escolha Monitoramento de runtime.
3. Na guia Configuração, escolha Editar.
4. Na seção EC2, escolha Habilitar.
5. Escolha Salvar.
6. Você pode verificar se a associação SSM GuardDuty criada instalará e gerenciará o agente de segurança em todos os recursos do EC2 pertencentes à sua conta.

    a. Abra o AWS Systems Manager console em https://console.aws.amazon.com/systems-manager/.

    b. Abra a guia Destinos da associação SSM (`GuardDutyRuntimeMonitoring-do-not-delete`). Observe que a chave Tag aparece como InstanceIds.

Using inclusion tag in selected instances

Para configurar o agente GuardDuty de segurança para instâncias selecionadas do Amazon EC2

1. Faça login no Console de gerenciamento da AWS e abra o console do Amazon EC2 em. https://console.aws.amazon.com/ec2/
2. Adicione a `true` tag`GuardDutyManaged`: às instâncias que você GuardDuty deseja monitorar e detectar possíveis ameaças. Para obter informações sobre como adicionar essa tag, consulte Para adicionar uma tag a um recurso individual.
3. Você pode verificar se a associação SSM GuardDuty criada instalará e gerenciará o agente de segurança somente nos recursos do EC2 que estão marcados com as tags de inclusão.

    Abra o AWS Systems Manager console em https://console.aws.amazon.com/systems-manager/.

- Abra a guia Destinos da associação SSM que é criada (`GuardDutyRuntimeMonitoring-do-not-delete`). A chave Tag aparece como tag: GuardDutyManaged.

Using exclusion tag in selected instances

> **Note**
>
> Certifique-se de adicionar a tag de exclusão às instâncias do Amazon EC2 antes de iniciá-las. Depois de habilitar a configuração automatizada do agente para o Amazon EC2, qualquer instância do EC2 que seja executada sem uma tag de exclusão será coberta GuardDuty pela configuração automática do agente.

Para configurar o agente GuardDuty de segurança para instâncias selecionadas do Amazon EC2

1. Faça login no Console de gerenciamento da AWS e abra o console do Amazon EC2 em. https://console.aws.amazon.com/ec2/
2. Adicione a `false` tag`GuardDutyManaged`: às instâncias que você não GuardDuty deseja monitorar e detectar possíveis ameaças. Para obter informações sobre como adicionar essa tag, consulte Para adicionar uma tag a um recurso individual.
3. Para o etiquetas de exclusão a serem disponibilizadas nos metadados da instância, execute as seguintes etapas:

   a. Na guia Detalhes da sua instância, veja o status de Permitir tags nos metadados da instância.

      Se estiver Desativado no momento, use as etapas a seguir para alterar o status para Ativado. Caso contrário, ignore essa etapa.

   b. Selecione a instância para a qual deseja permitir tags.

   c. No menu Ações, escolha Configurações da instância.

   d. Escolha Permitir tags em metadados de instância.

   e. Em Acesso a tags no metadados de instância, selecione Permitir.

   f. Escolha Salvar.

4. Depois de adicionar a tag de exclusão, execute as mesmas etapas especificadas na guia Configurar para todas as instâncias.

Agora você pode avaliar o runtime Cobertura de runtime e solução de problemas para instância do Amazon EC2.

Migração do agente manual do Amazon EC2 para o agente automatizado

Esta seção se aplica Conta da AWS se você já gerenciava o agente de segurança manualmente e agora deseja usar a configuração GuardDuty automatizada do agente. Se isso não se aplicar a você, continue configurando o agente de segurança da sua conta.

Quando você ativa o agente GuardDuty automatizado, GuardDuty gerencia o agente de segurança em seu nome. Para obter informações sobre quais etapas são GuardDuty necessárias, consulteConfiguração automatizada do agente (recomendada).

Limpar os recursos

Excluir uma associação SSM

- Exclua qualquer associação SSM que você possa ter criado ao gerenciar manualmente o agente de segurança do Amazon EC2. Para obter mais informações, consulte Excluindo associações.
- Isso é feito para que GuardDuty possa assumir o gerenciamento das ações de SSM, independentemente de você usar agentes automatizados no nível da conta ou da instância (usando tags de inclusão ou exclusão). Para obter mais informações sobre quais ações do SSM podem ser GuardDuty tomadas, consulteService-linked permissões de função para GuardDuty.
- Quando você exclui uma associação de SSM que foi criada anteriormente para gerenciar o agente de segurança manualmente, pode haver um breve período de sobreposição ao GuardDuty criar uma associação de SSM para gerenciar o agente de segurança automaticamente. Durante esse período, você pode enfrentar conflitos com base no agendamento do SSM. Para obter mais informações, consulte Programação de SSM do Amazon EC2.

Gerencie tags de inclusão e exclusão para suas instâncias do Amazon EC2

- Tags de inclusão — Quando você não ativa a configuração GuardDuty automática do agente, mas marca qualquer uma das suas instâncias do Amazon EC2 com uma tag de inclusão (`GuardDutyManaged:true`), GuardDuty cria uma associação SSM que instalará e gerenciará

o agente de segurança nas instâncias do EC2 selecionadas. Esse é um comportamento esperado que ajuda você a gerenciar o agente de segurança somente em instâncias EC2 selecionadas. Para obter mais informações, consulte Implantação do agente de segurança no Amazon EC2.

Para GuardDuty evitar a instalação e o gerenciamento do agente de segurança, remova a tag de inclusão dessas instâncias do EC2. Para obter mais informações, consulte Adicionar e excluir tags no Guia do usuário do Amazon EC2.

- Tags de exclusão — Quando você quiser habilitar a configuração GuardDuty automatizada do agente para todas as instâncias do EC2 em sua conta, certifique-se de que nenhuma instância do EC2 esteja marcada com uma tag de exclusão (:). `GuardDutyManaged` `false`

Gerenciando o agente de segurança manualmente para o recurso do Amazon EC2

Esta seção fornece as etapas para instalar e atualizar manualmente o agente de segurança para seus recursos do Amazon EC2.

Depois de ativar o Runtime Monitoring, você precisará instalar o agente GuardDuty de segurança manualmente. Para gerenciar o agente GuardDuty de segurança manualmente, primeiro você deve criar um endpoint da Amazon VPC manualmente. Depois disso, você pode instalar o agente de segurança para que ele comece GuardDuty a receber os eventos de tempo de execução das instâncias do Amazon EC2. Ao GuardDuty lançar uma nova versão do agente para esse recurso, você pode atualizar a versão do agente em sua conta.

Os tópicos a seguir incluem as etapas para gerenciar continuamente o agente de segurança dos seus recursos do Amazon EC2.

Tópicos

- Pré-requisito — Criando um endpoint da Amazon VPC manualmente
- Instalando o agente de segurança manualmente
- Atualização manual do agente GuardDuty de segurança para a instância do Amazon EC2

Pré-requisito — Criando um endpoint da Amazon VPC manualmente

Antes de instalar o agente de GuardDuty segurança, você deve criar um endpoint da Amazon Virtual Private Cloud (Amazon VPC). Isso ajudará a GuardDuty receber os eventos de tempo de execução de suas instâncias do Amazon EC2.

> **Note**
>
> Não há custo adicional para usar o endpoint da VPC.

Para criar um endpoint da VPC do Amazon

1. Faça login no Console de gerenciamento da AWS e abra o console da Amazon VPC em. https://console.aws.amazon.com/vpc/
2. No painel de navegação, em Nuvem privada VPC, escolha Endpoints.
3. Escolha Criar endpoint.
4. Na página Criar endpoint, para a Categoria de serviço, escolha Outros serviços de endpoint.
5. Em Nome do serviço, digite **`com.amazonaws.`*`us-east-1`*`.guardduty-data`**.

   Certifique-se de substituir *`us-east-1`* por seu Região da AWS. Essa deve ser a mesma região da instância do Amazon EC2 que pertence ao ID da sua AWS conta.
6. Selecione Verificar serviço.
7. Depois que o nome do serviço for verificado com sucesso, escolha a VPC em que reside sua instância. Adicione a política a seguir para restringir o uso do endpoint da Amazon VPC somente à conta especificada. Com a `Condition` da organização fornecida abaixo desta política, você pode atualizar a política a seguir para restringir o acesso ao seu endpoint. Para fornecer suporte de endpoint da Amazon VPC para IDs de conta específicos em sua organização, consulte Organization condition to restrict access to your endpoint.

   JSON

```
{
 "Version":"2012-10-17",
 "Statement": [
  {
   "Action": "*",
```

```
    "Resource": "*",
    "Effect": "Allow",
    "Principal": "*"
   },
   {
    "Condition": {
     "StringNotEquals": {
      "aws:PrincipalAccount": "111122223333"
     }
    },
    "Action": "*",
    "Resource": "*",
    "Effect": "Deny",
    "Principal": "*"
   }
  ]
}
```

O ID de conta `aws:PrincipalAccount` deve corresponder à conta que contém a VPC e o endpoint da VPC. A lista a seguir mostra como compartilhar o VPC endpoint com outros AWS IDs de conta:

- Para especificar várias contas para acessar o endpoint da VPC, substitua `"aws:PrincipalAccount: "111122223333"` pelo seguinte bloco:

  ```
  "aws:PrincipalAccount": [
            "666666666666",
            "555555555555"
       ]
  ```

  Certifique-se de substituir os AWS IDs da conta pelos IDs das contas que precisam acessar o VPC endpoint.

- Para permitir que todos os membros de uma organização acessem o endpoint da VPC, substitua `"aws:PrincipalAccount: "111122223333"` pela seguinte linha:

  ```
  "aws:PrincipalOrgID": "o-abcdef0123"
  ```

  Certifique-se de substituir a organização *o-abcdef0123* pelo ID da organização.

- Para restringir o acesso para um recurso a um ID de organização, adicione seu `ResourceOrgID` à política. Para obter mais informações, consulte `aws:ResourceOrgID` no Guia do usuário do IAM.

```
"aws:ResourceOrgID": "o-abcdef0123"
```

8. Em Configurações adicionais, selecione Habilitar nome DNS.
9. Em Sub-redes, escolha as sub-redes em que reside sua instância.
10. Em Grupos de segurança, escolha um grupo de segurança que tenha a porta de entrada 443 habilitada em sua VPC (ou em sua instância do Amazon EC2). Se você ainda não tem um grupo de segurança que tenha uma porta de entrada 443 habilitada, consulte Criar um grupo de segurança para sua VPC no Guia do usuário da Amazon VPC.

    Se houver um problema ao restringir as permissões de entrada para sua VPC (ou instância), é possível usar a porta de entrada 443 de qualquer endereço IP (`0.0.0.0/0`). No entanto, GuardDuty recomenda o uso de endereços IP que correspondam ao bloco CIDR da sua VPC. Para obter mais informações, consulte Blocos VPC CIDR no Guia do usuário da Amazon VPC.

Depois de seguir as etapas, verifique em Validando a configuração do endpoint da VPC se o endpoint da VPC foi configurado corretamente.

Instalando o agente de segurança manualmente

GuardDuty fornece os dois métodos a seguir para instalar o agente GuardDuty de segurança em suas instâncias do Amazon EC2. Antes de continuar, certifique-se de seguir as etapas em Pré-requisito — Criando um endpoint da Amazon VPC manualmente.

Escolha um método de acesso preferencial para instalar o agente de segurança em seus recursos do Amazon EC2.

- Método 1 - Usando AWS Systems Manager— Esse método exige que sua instância do Amazon EC2 seja AWS Systems Manager gerenciada.
- Método 2 - Usando Linux Package Managers— Você pode usar esse método independentemente de suas instâncias do Amazon EC2 serem AWS Systems Manager gerenciadas ou não. Com base nas distribuições do seu sistema operacional, escolha um método apropriado para instalar scripts RPM ou Debian. Se você usa a plataforma Fedora, deve usar esse método para instalar o agente.

Método 1 - Usando AWS Systems Manager

Para usar esse método, certifique-se de que suas instâncias do Amazon EC2 sejam AWS Systems Manager gerenciadas e, em seguida, instale o agente.

AWS Systems Manager instância gerenciada do Amazon EC2

Use as seguintes etapas para que as instâncias do Amazon EC2 sejam gerenciadas por AWS Systems Manager .

- AWS Systems Manager ajuda você a gerenciar seus AWS aplicativos e recursos de ponta a ponta e possibilita operações seguras em grande escala.

  Para gerenciar suas instâncias do Amazon EC2 com AWS Systems Manager, consulte Configurando o Systems Manager para instâncias do Amazon EC2 no AWS Systems Manager Guia do usuário.
- A tabela a seguir mostra os novos AWS Systems Manager documentos GuardDuty gerenciados:

Nome do documento	Tipo de documento	Finalidade
`AmazonGuardDuty-RuntimeMonitoringSsmPlugin`	Distribuidor	Para empacotar o agente GuardDuty de segurança.
`AmazonGuardDuty-ConfigureRuntimeMonitoringSsmPlugin`	Command	Para executar o script installation/un -installation para instalar o agente GuardDuty de segurança.

Para obter mais informações sobre AWS Systems Manager, consulte os documentos do Amazon EC2 Systems Manager no Guia AWS Systems Manager do usuário.

> **Para servidores Debian**
>
> As Amazon Machine Images (AMIs) para o Debian Server fornecidas por AWS exigem que você instale o AWS Systems Manager agente (agente SSM). Você precisará realizar uma etapa adicional para instalar o agente SSM para tornar suas instâncias do Amazon EC2 Debian Server gerenciadas por SSM. Para obter informações sobre as etapas que você

precisa seguir, consulte Instalando manualmente o agente SSM nas instâncias do servidor Debian no AWS Systems Manager Guia do Usuário.

Para instalar o GuardDuty agente para a instância do Amazon EC2 usando AWS Systems Manager

1. Abra o AWS Systems Manager console em https://console.aws.amazon.com/systems-manager/.
2. No painel de navegação, escolha Documentos
3. Em Propriedade da Amazon, escolha `AmazonGuardDuty-ConfigureRuntimeMonitoringSsmPlugin`.
4. Escolha Run Command.
5. Insira os seguintes parâmetros Run Command
   - Ação: escolha Instalar.
   - Tipo de instalação: escolha Instalar ou Desinstalar.
   - Nome: `AmazonGuardDuty-RuntimeMonitoringSsmPlugin`
   - Versão: se ela permanecer vazia, você receberá a versão mais recente do agente de GuardDuty segurança. Para obter mais informações sobre as versões de lançamento, GuardDuty versões do agente de segurança para instâncias do Amazon EC2.
6. Selecione a instância do Amazon EC2 de destino. Você pode selecionar uma ou mais instâncias do Amazon EC2. Para obter mais informações, consulte AWS Systems Manager Executando comandos do console no AWS Systems Manager Guia do usuário
7. Valide se a instalação do GuardDuty agente está íntegra. Para obter mais informações, consulte Validando o status GuardDuty de instalação do agente de segurança.

Método 2 - Usando Linux Package Managers

Com esse método, você pode instalar o agente GuardDuty de segurança executando scripts RPM ou scripts Debian. Com base nos sistemas operacionais, selecione um método de sua preferência:

- Use scripts RPM para instalar o agente de segurança nas distribuições do sistema operacional AL2, AL2023, RedHat CentOS ou Fedora.
- Use scripts Debian para instalar o agente de segurança nas distribuições do sistema operacional Ubuntu ou Debian. Para obter informações sobre as distribuições suportadas dos sistemas operacionais Ubuntu e Debian, consulte Validação dos requisitos de arquitetura.

RPM installation

> **Important**
>
> Recomendamos verificar a assinatura RPM do agente de GuardDuty segurança antes de instalá-la em sua máquina.

1. Verifique a assinatura RPM do agente de GuardDuty segurança

   a. Prepare o modelo

   Prepare os comandos com a chave pública apropriada, assinatura de x86_64 RPM, assinatura de arm64 RPM e o link de acesso correspondente aos scripts de RPM hospedados nos buckets do Amazon S3. Substitua o valor do Região da AWS ID da AWS conta e a versão do GuardDuty agente para acessar os scripts de RPM.

   - Chave pública:

     ```
     s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.17.1/
     publickey.pem
     ```

   - GuardDuty assinatura RPM do agente de segurança:

     Assinatura de x86_64 RPM

     ```
     s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.17.1/
     x86_64/amazon-guardduty-agent-1.17.1.x86_64.sig
     ```

     Assinatura de arm64 RPM

     ```
     s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.17.1/arm64/
     amazon-guardduty-agent-1.17.1.arm64.sig
     ```

   - Acesse os links para os scripts de RPM no bucket do Amazon S3:

     Link de acesso para x86_64 RPM

     ```
     s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.17.1/
     x86_64/amazon-guardduty-agent-1.17.1.x86_64.rpm
     ```

Link de acesso para arm64 RPM

```
s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.17.1/arm64/
amazon-guardduty-agent-1.17.1.arm64.rpm
```

Região da AWS	Nome da região	AWS ID da conta
eu-west-1	Europa (Irlanda)	694911143906
us-east-1	Leste dos EUA (Norte da Virgínia)	593207742271
us-west-2	Oeste dos EUA (Oregon)	733349766148
eu-west-3	Europa (Paris)	665651866788
us-east-2	Leste dos EUA (Ohio)	307168627858
eu-central-1	Europa (Frankfurt)	323658145986
ap-northeast-2	Ásia-Pacífico (Seul)	914738172881
eu-north-1	Europa (Estocolmo)	591436053604
ap-east-1	Ásia-Pacífico (Hong Kong)	258348409381
me-south-1	Oriente Médio (Bahrein)	536382113932
eu-west-2	Europa (Londres)	892757235363
ap-northeast-1	Ásia-Pacífico (Tóquio)	533107202818
ap-southeast-1	Ásia-Pacífico (Singapura)	174946120834
ap-south-1	Ásia-Pacífico (Mumbai)	251508486986
ap-southeast-3	Ásia-Pacífico (Jacarta)	510637619217

sa-east-1	América do Sul (São Paulo)	758426053663
ap-northeast-3	Ásia-Pacífico (Osaka)	273192626886
eu-south-1	Europa (Milão)	266869475730
af-south-1	África (Cidade do Cabo)	197869348890
ap-southeast-2	Ásia-Pacífico (Sydney)	00:5257.825.471
me-central-1	Oriente Médio (Emirados Árabes Unidos)	00:00:1452.1398
us-west-1	Oeste dos EUA (N. da Califórnia)	684579721401
ca-central-1	Canadá (Central)	354763396469
ca-west-1	Oeste do Canadá (Calgary)	339712888787
ap-south-2	Ásia-Pacífico (Hyderabad)	950823858135
eu-south-2	Europa (Espanha)	919611009337
eu-central-2	Europa (Zurique)	529164026651
ap-southeast-4	Ásia-Pacífico (Melbourne)	251357961535
ap-southeast-7	Ásia-Pacífico (Tailândia)	054037130133
il-central-1	Israel (Tel Aviv)	870907303882
mx-central-1	México (Centro)	982081086614
ap-east-2	Ásia-Pacífico (Taipei)	259886477082

b. Faça download do modelo

No comando a seguir, para baixar a chave pública apropriada, a assinatura de x86_64 RPM, a assinatura de arm64 RPM e o link de acesso correspondente aos scripts de

RPM hospedados nos buckets do Amazon S3, certifique-se de substituir o ID da conta pelo ID Conta da AWS apropriado e a região pela sua região atual.

```
aws s3 cp s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.17.1/
x86_64/amazon-guardduty-agent-1.17.1.x86_64.rpm ./amazon-guardduty-
agent-1.17.1.x86_64.rpm
aws s3 cp s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.17.1/
x86_64/amazon-guardduty-agent-1.17.1.x86_64.sig ./amazon-guardduty-
agent-1.17.1.x86_64.sig
aws s3 cp s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.17.1/
publickey.pem ./publickey.pem
```

c. Importar a chave pública

Use o comando a seguir para importar a chave pública para o banco de dados:

```
gpg --import publickey.pem
```

gpg mostra a importação executada com sucesso

```
gpg: key 093FF49D: public key "AwsGuardDuty" imported
gpg: Total number processed: 1
gpg:               imported: 1  (RSA: 1)
```

d. Verifique a assinatura

Use o seguinte comando para verificar a assinatura

```
gpg --verify amazon-guardduty-agent-1.17.1.x86_64.sig amazon-guardduty-
agent-1.17.1.x86_64.rpm
```

Caso a verificação seja aprovada, será exibida uma mensagem semelhante ao resultado abaixo. Agora você pode prosseguir com a instalação do agente GuardDuty de segurança usando o RPM.

Resultado do exemplo:

```
gpg: Signature made Fri 17 Nov 2023 07:58:11 PM UTC using ? key ID 093FF49D
gpg: Good signature from "AwsGuardDuty"
gpg: WARNING: This key is not certified with a trusted signature!
```

```
gpg:          There is no indication that the signature belongs to the
 owner.
Primary key fingerprint: 7478 91EF 5378 1334 4456  7603 06C9 06A7 093F F49D
```

Caso ocorra uma falha na verificação, isso significa que a assinatura no RPM foi possivelmente adulterada. Remova a chave pública do banco de dados e repita o processo de verificação.

Exemplo:

```
gpg: Signature made Fri 17 Nov 2023 07:58:11 PM UTC using ? key ID 093FF49D
gpg: BAD signature from "AwsGuardDuty"
```

Use o seguinte comando para remover a chave pública do banco de dados:

```
gpg --delete-keys AwsGuardDuty
```

Agora, tente o processo de verificação novamente.

2. Conectar com SSH via macOS ou Linux
3. Instale o agente de GuardDuty segurança usando o seguinte comando:

```
sudo rpm -ivh amazon-guardduty-agent-1.17.1.x86_64.rpm
```

4. Valide se a instalação do GuardDuty agente está íntegra. Para mais informações sobre essas etapas, consulte Validando o status GuardDuty de instalação do agente de segurança.

Debian installation

> **Important**
>
> Recomendamos verificar a assinatura do agente GuardDuty de segurança Debian antes de instalá-la em sua máquina.

1. Verifique a assinatura do agente de GuardDuty segurança Debian

a. Prepare modelos para a chave pública apropriada, assinatura do pacote Debian amd64, assinatura do pacote Debian arm64 e o link de acesso correspondente aos scripts Debian hospedados nos buckets do Amazon S3

   Nos modelos a seguir, substitua o valor do Região da AWS, ID da AWS conta e a versão do GuardDuty agente para acessar os scripts do pacote Debian.

   - Chave pública:

     ```
     s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.17.1/
     publickey.pem
     ```

   - GuardDuty assinatura Debian do agente de segurança:

     Assinatura de amd64

     ```
     s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.17.1/amd64/
     amazon-guardduty-agent-1.17.1.amd64.sig
     ```

     Assinatura de arm64

     ```
     s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.17.1/arm64/
     amazon-guardduty-agent-1.17.1.arm64.sig
     ```

   - Acesse os links para os scripts de Debian no bucket Amazon S3:

     Link de acesso para o amd64

     ```
     s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.17.1/amd64/
     amazon-guardduty-agent-1.17.1.amd64.deb
     ```

     Link de acesso para arm64

     ```
     s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.17.1/arm64/
     amazon-guardduty-agent-1.17.1.arm64.deb
     ```

Região da AWS	Nome da região	AWS ID da conta
eu-west-1	Europa (Irlanda)	694911143906

us-east-1	Leste dos EUA (Norte da Virgínia)	593207742271
us-west-2	Oeste dos EUA (Oregon)	733349766148
eu-west-3	Europa (Paris)	665651866788
us-east-2	Leste dos EUA (Ohio)	307168627858
eu-central-1	Europa (Frankfurt)	323658145986
ap-northeast-2	Ásia-Pacífico (Seul)	914738172881
eu-north-1	Europa (Estocolmo)	591436053604
ap-east-1	Ásia-Pacífico (Hong Kong)	258348409381
me-south-1	Oriente Médio (Bahrein)	536382113932
eu-west-2	Europa (Londres)	892757235363
ap-northeast-1	Ásia-Pacífico (Tóquio)	533107202818
ap-southeast-1	Ásia-Pacífico (Singapura)	174946120834
ap-south-1	Ásia-Pacífico (Mumbai)	251508486986
ap-southeast-3	Ásia-Pacífico (Jacarta)	510637619217
sa-east-1	América do Sul (São Paulo)	758426053663
ap-northeast-3	Ásia-Pacífico (Osaka)	273192626886
eu-south-1	Europa (Milão)	266869475730
af-south-1	África (Cidade do Cabo)	197869348890
ap-southeast-2	Ásia-Pacífico (Sydney)	00:5257.825.471

me-central-1	Oriente Médio (Emirados Árabes Unidos)	00:00:1452.1398
us-west-1	Oeste dos EUA (N. da Califórnia)	684579721401
ca-central-1	Canadá (Central)	354763396469
ca-west-1	Oeste do Canadá (Calgary)	339712888787
ap-south-2	Ásia-Pacífico (Hyderabad)	950823858135
eu-south-2	Europa (Espanha)	919611009337
eu-central-2	Europa (Zurique)	529164026651
ap-southeast-4	Ásia-Pacífico (Melbourne)	251357961535
il-central-1	Israel (Tel Aviv)	870907303882
mx-central-1	México (Centro)	982081086614
ap-east-2	Ásia-Pacífico (Taipei)	259886477082

b. Baixe a chave pública apropriada, assinatura de amd64, assinatura de arm64 e o link de acesso correspondente para os scripts do Debian hospedados nos buckets do Amazon S3

   Nos comandos a seguir, substitua o ID da conta pelo Conta da AWS ID apropriado e a Região pela sua região atual.

```
aws s3 cp s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.17.1/
amd64/amazon-guardduty-agent-1.17.1.amd64.deb ./amazon-guardduty-
agent-1.17.1.amd64.deb
aws s3 cp s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.17.1/
amd64/amazon-guardduty-agent-1.17.1.amd64.sig ./amazon-guardduty-
agent-1.17.1.amd64.sig
aws s3 cp s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.17.1/
publickey.pem ./publickey.pem
```

c. Importar a chave pública para o banco de dados

```
gpg --import publickey.pem
```

gpg mostra a importação com sucesso

```
gpg: key 093FF49D: public key "AwsGuardDuty" imported
gpg: Total number processed: 1
gpg:               imported: 1  (RSA: 1)
```

d. Verifique a assinatura

```
gpg --verify amazon-guardduty-agent-1.17.1.amd64.sig amazon-guardduty-
agent-1.17.1.amd64.deb
```

Após uma verificação bem-sucedida, você verá uma mensagem semelhante ao seguinte resultado:

Resultado do exemplo:

```
gpg: Signature made Fri 17 Nov 2023 07:58:11 PM UTC using ? key ID 093FF49D
gpg: Good signature from "AwsGuardDuty"
gpg: WARNING: This key is not certified with a trusted signature!
gpg:          There is no indication that the signature belongs to the
 owner.
Primary key fingerprint: 7478 91EF 5378 1334 4456  7603 06C9 06A7 093F F49D
```

Agora você pode prosseguir com a instalação do agente GuardDuty de segurança usando o Debian.

No entanto, se a verificação falhar, isso significa que a assinatura no pacote Debian foi potencialmente adulterada.

Exemplo:

```
gpg: Signature made Fri 17 Nov 2023 07:58:11 PM UTC using ? key ID 093FF49D
gpg: BAD signature from "AwsGuardDuty"
```

Use o seguinte comando para remover a chave pública do banco de dados:

```
gpg --delete-keys AwsGuardDuty
```

Agora, repita o processo de verificação.

2. Conectar com SSH via macOS ou Linux
3. Instale o agente de GuardDuty segurança usando o seguinte comando:

```
sudo dpkg -i amazon-guardduty-agent-1.17.1.amd64.deb
```

4. Valide se a instalação do GuardDuty agente está íntegra. Para mais informações sobre essas etapas, consulte Validando o status GuardDuty de instalação do agente de segurança.

Erros de falta de memória.

Se você tiver um `out-of-memory` erro ao instalar ou atualizar manualmente o agente GuardDuty de segurança do Amazon EC2, consulte. Solução de problemas de falta de memória

Validando o status GuardDuty de instalação do agente de segurança

Depois de executar as etapas para instalar o agente GuardDuty de segurança, use as etapas a seguir para validar o status do agente:

Para validar se o agente de GuardDuty segurança está íntegro

1. Conectar com SSH via macOS ou Linux
2. Execute o comando a seguir para verificar o status do agente GuardDuty de segurança:

```
sudo systemctl status amazon-guardduty-agent
```

Se quiser ver os logs de instalação do agente de segurança, eles estão disponíveis em `/var/log/amzn-guardduty-agent/`.

Para exibir os logs, execute `sudo journalctl -u amazon-guardduty-agent`.

Atualização manual do agente GuardDuty de segurança para a instância do Amazon EC2

GuardDuty lança atualizações para as versões do agente de segurança. Ao gerenciar o agente de segurança manualmente, você é responsável por atualizar o agente para suas instâncias do

Amazon EC2. Para obter informações sobre novas versões de agente, consulte GuardDuty versões de lançamento do agente de segurança para instâncias do Amazon EC2. Para receber notificações sobre o lançamento de uma nova versão do agente, consulte Inscrever-se para receber anúncios do Amazon GuardDuty SNS.

Para atualizar manualmente o agente de segurança para instância do Amazon EC2

O processo para atualizar o agente de segurança é o mesmo que instalar o agente de segurança. Dependendo do método que você usou para instalar o agente, você pode executar as etapas em Instalando o agente de segurança manualmente para instâncias do Amazon EC2.

Se você usar o Método 1 - Usando AWS Systems Manager, poderá atualizar o agente de segurança usando o comando Executar. Use a versão do agente para a qual você deseja atualizar.

Se usar o Método 2 - Usando Linux Package Managers, você pode usar os scripts conforme especificado na seção Instalando o agente de segurança manualmente. Os scripts já incluem a versão mais recente de lançamento do agente. Para obter informações sobre as versões do agente recentemente lançadas, consulte GuardDuty versões do agente de segurança para instâncias do Amazon EC2.

Depois de atualizar o agente de segurança, você pode verificar o status da instalação examinando os logs. Para obter mais informações, consulte Validando o status GuardDuty de instalação do agente de segurança.

Gerenciando o agente GuardDuty de segurança no Bottlerocket (Amazon ECS no Amazon EC2)

Important

Esta página se aplica somente à versão das ECS-optimized AMIs do Bottlerocket `v1.62.1` e posteriores, incluindo as seguintes variantes:

- `bottlerocket-aws-ecs-2-x86_64` / `bottlerocket-aws-ecs-2-aarch64`
- `bottlerocket-aws-ecs-3-x86_64` / `bottlerocket-aws-ecs-3-aarch64`
- `bottlerocket-aws-ecs-2-nvidia` / `bottlerocket-aws-ecs-2-nvidia-fips`
- `bottlerocket-aws-ecs-3-nvidia` / `bottlerocket-aws-ecs-3-nvidia-fips`

Para instâncias do Bottlerocket nos clusters do Amazon EKS, o Runtime Monitoring usa uma configuração diferente. Consulte Pré-requisitos para o suporte ao cluster do Amazon EKS.

Esta página explica como o agente de GuardDuty segurança é executado nas ECS-optimized AMIs do Bottlerocket e como o implanta. GuardDuty No Bottlerocket, o agente é executado como um contêiner host e não como um pacote RPM ou Debian instalado. O Bottlerocket é um sistema operacional Linux otimizado para contêineres com um sistema de arquivos raiz imutável, portanto, não usa gerenciadores de pacotes tradicionais. GuardDuty hospeda a imagem do contêiner do agente em um repositório do Amazon Elastic Container Registry (Amazon ECR) que ele gerencia e, quando você ativa o Runtime Monitoring com a configuração automatizada do agente GuardDuty , AWS Systems Manager usa o Distributor para implantar o contêiner do agente host para você.

Pré-requisitos

Antes de continuar, verifique se todas Pré-requisitos para o suporte do Bottlerocket ECS-EC2 foram seguidas.

Habilitando a configuração automatizada do agente

ECS-EC2 As instâncias do Bottlerocket usam o mesmo documento SSM e a mesma configuração automatizada de agentes das instâncias padrão do Amazon EC2. Para habilitar o agente GuardDuty automatizado para suas instâncias do Bottlerocket, siga as etapas em. Atendente automatizado no recurso Amazon EC2 Isso inclui:

- Habilitando o GuardDuty agente em um ambiente com várias contas.
- Habilitando o agente GuardDuty automatizado em uma conta independente.

Para obter pré-requisitos adicionais ao usar tags de inclusão ou exclusão, consulte. Ao usar a configuração de agente automatizado

Verificando o agente

Depois de ativar a configuração automatizada do agente, verifique se o agente está em execução na sua instância do Bottlerocket:

1. Conecte-se à sua instância usando o SSM Session Manager.

2. Entre no contêiner de administração:`enter-admin-container`.
3. Verifique os registros do agente usando uma das seguintes opções:
   - `sheltie journalctl -u host-containers@amazon-guardduty-agent`
   - De uma sessão do Sheltie (`sudo sheltie`):`ls /var/log/amzn-guardduty-agent/`.

Para obter informações sobre a revisão das estatísticas de cobertura de suas instâncias do Amazon EC2, consulte. Análise de estatísticas de cobertura

Se o status da cobertura for exibido como Não íntegro, consulteSolução de problemas de cobertura de tempo de execução do Bottlerocket ECS-EC2.

Gerenciamento de agente de segurança automatizado para Fargate (somente Amazon ECS)

O Runtime Monitoring suporta o gerenciamento do agente de segurança para seus clusters do Amazon ECS (AWS Fargate) somente por meio GuardDuty de. Não há suporte para gerenciar o agente de segurança manualmente nos clusters do Amazon ECS.

Antes de prosseguir com as etapas nesta seção, certifique-se de seguir Pré-requisitos para AWS Fargate Suporte (somente para Amazon ECS).

Com base nas abordagens emImplantação do agente de segurança no Amazon ECS no Fargate, escolha um método preferido para habilitar o agente GuardDuty automatizado para seus recursos.

Configurando o GuardDuty agente para um ambiente com várias contas

Em um ambiente de várias contas, somente a conta de GuardDuty administrador delegado pode habilitar ou desabilitar a configuração automática de agentes para as contas membros e gerenciar a configuração automática de agentes para clusters do Amazon ECS que pertencem às contas membros em sua organização. Uma conta de GuardDuty membro não pode modificar essa configuração. A conta de GuardDuty administrador delegado gerencia suas contas de membros usando AWS Organizations. Para obter mais informações sobre ambientes com várias contas, consulte Gerenciando várias contas em GuardDuty.

Habilitando a configuração automatizada do agente para a conta de GuardDuty administrador delegado

Manage for all Amazon ECS clusters (account level)

Se você escolher Habilitar para todas as contas para Monitoramento de runtime, terá as seguintes opções:

- Escolha Ativar para todas as contas na seção Configuração automática do agente. GuardDuty implantará e gerenciará o agente de segurança para todas as tarefas do Amazon ECS que forem lançadas.
- Escolha Configurar contas manualmente.

Se você escolheu Configurar contas manualmente na seção Monitoramento de runtime, faça o seguinte:

1. Selecione Configurar contas manualmente na seção Configuração de agente automatizado.
2. Escolha Habilitar na seção Conta de GuardDuty administrador delegado (esta conta).

Escolha Salvar.

Quando você GuardDuty deseja monitorar tarefas que fazem parte de um serviço, é necessária a implantação de um novo serviço após a ativação do Runtime Monitoring. Se a última implantação de um serviço ECS específico foi iniciada antes de você habilitar o Monitoramento de runtime, você pode reiniciar o serviço ou atualizar o serviço usando `forceNewDeployment`.

Nas etapas de atualização do serviço, consulte os seguintes recursos:

- Atualização de um serviço Amazon ECS usando o console no Guia do desenvolvedor Amazon Elastic Container Service.
- UpdateServicena Referência de API do Amazon Elastic Container Service.
- update-service na Referência de comando da AWS CLI .

Manage for all Amazon ECS clusters but exclude some of the clusters (cluster level)

1. Adicione uma tag a esse cluster do Amazon ECS com o par chave-valor como `GuardDutyManaged-false`.

2. Impeça a modificação de tags, exceto pelas entidades confiáveis. A política fornecida em Impedir que as tags sejam modificadas, exceto pelos princípios autorizados no Guia do usuário AWS Organizations foi modificada para ser aplicável aqui.

   JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:TagResource",
                "ecs:UntagResource"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "ecs:ResourceTag/GuardDutyManaged":
 "${aws:PrincipalTag/GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "Null": {
                    "ecs:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:TagResource",
                "ecs:UntagResource"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
```

```
                "StringNotEquals": {
                    "aws:RequestTag/GuardDutyManaged":
 "${aws:PrincipalTag/GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyManaged"
                    ]
                }
            }
        },
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
            "Action": [
                "ecs:TagResource",
                "ecs:UntagResource"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
            }
        }
    ]
}
```

3. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.
4. No painel de navegação, escolha Monitoramento de runtime.
5.

> **Note**
>
> Sempre adicione a tag de exclusão aos seus clusters do Amazon ECS antes de ativar a configuração automática do agente para sua conta; caso contrário, o

contêiner GuardDuty auxiliar será anexado a todos os contêineres nas tarefas do Amazon ECS que forem iniciadas.

Na guia Configuração, escolha Habilitar na Configuração do automatizada do agente.

Para os clusters do Amazon ECS que não foram excluídos, GuardDuty gerenciaremos a implantação do agente de segurança no contêiner auxiliar.

6. Escolha Salvar.
7. Quando você GuardDuty deseja monitorar tarefas que fazem parte de um serviço, é necessária a implantação de um novo serviço após a ativação do Runtime Monitoring. Se a última implantação de um serviço ECS específico foi iniciada antes de você habilitar o Monitoramento de runtime, você pode reiniciar o serviço ou atualizar o serviço usando `forceNewDeployment`.

   Nas etapas de atualização do serviço, consulte os seguintes recursos:

   - Atualização de um serviço Amazon ECS usando o console no Guia do desenvolvedor Amazon Elastic Container Service.
   - UpdateServicena Referência de API do Amazon Elastic Container Service.
   - update-service na Referência de comando da AWS CLI .

Manage for selective (inclusion only) Amazon ECS clusters (cluster level)

1. Adicione uma tag a um cluster do Amazon ECS para o qual você deseja incluir todas as tarefas. O par chave-valor deve ser `GuardDutyManaged-true`.
2. Impeça a modificação dessas tags, exceto pelas entidades confiáveis. A política fornecida em Impedir que as tags sejam modificadas, exceto pelos princípios autorizados no Guia do usuário AWS Organizations foi modificada para ser aplicável aqui.

   JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
```

```
            "Effect": "Deny",
            "Action": [
                "ecs:TagResource",
                "ecs:UntagResource"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "ecs:ResourceTag/GuardDutyManaged":
 "${aws:PrincipalTag/GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "Null": {
                    "ecs:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:TagResource",
                "ecs:UntagResource"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/GuardDutyManaged":
 "${aws:PrincipalTag/GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyManaged"
                    ]
                }
            }
        },
```

```
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
            "Action": [
                "ecs:TagResource",
                "ecs:UntagResource"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
            }
        }
    ]
}
```

> **Note**
>
> Ao usar tags de inclusão para seus clusters do Amazon ECS, você não precisa habilitar explicitamente o GuardDuty agente por meio da configuração automática do agente.

3. Quando você GuardDuty deseja monitorar tarefas que fazem parte de um serviço, é necessária a implantação de um novo serviço após a ativação do Runtime Monitoring. Se a última implantação de um serviço ECS específico foi iniciada antes de você habilitar o Monitoramento de runtime, você pode reiniciar o serviço ou atualizar o serviço usando `forceNewDeployment`.

   Nas etapas de atualização do serviço, consulte os seguintes recursos:

   - Atualização de um serviço Amazon ECS usando o console no Guia do desenvolvedor Amazon Elastic Container Service.
   - UpdateServicena Referência de API do Amazon Elastic Container Service.

- update-service na Referência de comando da AWS CLI .

Auto-enable para todas as contas de membros

Manage for all Amazon ECS clusters (account level)

As etapas a seguir pressupõem que você escolheu Habilitar para todas as contas na seção Monitoramento de runtime.

1. Escolha Ativar para todas as contas na seção Configuração automática do agente. GuardDuty implantará e gerenciará o agente de segurança para todas as tarefas do Amazon ECS que forem lançadas.
2. Escolha Salvar.
3. Quando você GuardDuty deseja monitorar tarefas que fazem parte de um serviço, é necessária a implantação de um novo serviço após a ativação do Runtime Monitoring. Se a última implantação de um serviço ECS específico foi iniciada antes de você habilitar o Monitoramento de runtime, você pode reiniciar o serviço ou atualizar o serviço usando `forceNewDeployment`.

   Nas etapas de atualização do serviço, consulte os seguintes recursos:

   - Atualização de um serviço Amazon ECS usando o console no Guia do desenvolvedor Amazon Elastic Container Service.
   - UpdateServicena Referência de API do Amazon Elastic Container Service.
   - update-service na Referência de comando da AWS CLI .

Manage for all Amazon ECS clusters but exclude some of the clusters (cluster level)

1. Adicione uma tag a esse cluster do Amazon ECS com o par chave-valor como `GuardDutyManaged-false`.
2. Impeça a modificação de tags, exceto pelas entidades confiáveis. A política fornecida em Impedir que as tags sejam modificadas, exceto pelos princípios autorizados no Guia do usuário AWS Organizations foi modificada para ser aplicável aqui.

   JSON

```
{
```

```
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:TagResource",
                "ecs:UntagResource"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "ecs:ResourceTag/GuardDutyManaged":
 "${aws:PrincipalTag/GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "Null": {
                    "ecs:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:TagResource",
                "ecs:UntagResource"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/GuardDutyManaged":
 "${aws:PrincipalTag/GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyManaged"
```

```
                    ]
                }
            }
        },
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
            "Action": [
                "ecs:TagResource",
                "ecs:UntagResource"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
            }
        }
    ]
}
```

3. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.
4. No painel de navegação, escolha Monitoramento de runtime.
5.

> **Note**
>
> Sempre adicione a tag de exclusão aos seus clusters do Amazon ECS antes de ativar a configuração automática do agente para sua conta; caso contrário, o contêiner GuardDuty auxiliar será anexado a todos os contêineres nas tarefas do Amazon ECS que forem iniciadas.

   Na guia Configuração, escolha Editar.
6. Escolha Habilitar para todas as contas na seção Configuração automatizada do agente

Para os clusters do Amazon ECS que não foram excluídos, GuardDuty gerenciaremos a implantação do agente de segurança no contêiner auxiliar.

7. Escolha Salvar.
8. Quando você GuardDuty deseja monitorar tarefas que fazem parte de um serviço, é necessária a implantação de um novo serviço após a ativação do Runtime Monitoring. Se a última implantação de um serviço ECS específico foi iniciada antes de você habilitar o Monitoramento de runtime, você pode reiniciar o serviço ou atualizar o serviço usando `forceNewDeployment`.

   Nas etapas de atualização do serviço, consulte os seguintes recursos:

   - Atualização de um serviço Amazon ECS usando o console no Guia do desenvolvedor Amazon Elastic Container Service.
   - UpdateServicena Referência de API do Amazon Elastic Container Service.
   - update-service na Referência de comando da AWS CLI .

Manage for selective (inclusion-only) Amazon ECS clusters (cluster level)

Independentemente de como você escolhe habilitar o Monitoramento de runtime, as seguintes etapas ajudarão a monitorar as tarefas seletivas do Amazon ECS Fargate para todas as contas-membro na sua organização.

1. Não habilite nenhuma configuração na seção Configuração de agente automatizado Mantenha a configuração do Monitoramento de runtime igual à selecionada na etapa anterior.
2. Escolha Salvar.
3. Impeça a modificação dessas tags, exceto pelas entidades confiáveis. A política fornecida em Impedir que as tags sejam modificadas, exceto pelos princípios autorizados no Guia do usuário AWS Organizations foi modificada para ser aplicável aqui.

   JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
```

```
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:TagResource",
                "ecs:UntagResource"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "ecs:ResourceTag/GuardDutyManaged":
 "${aws:PrincipalTag/GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "Null": {
                    "ecs:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:TagResource",
                "ecs:UntagResource"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/GuardDutyManaged":
 "${aws:PrincipalTag/GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyManaged"
                    ]
                }
            }
```

```
        },
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
            "Action": [
                "ecs:TagResource",
                "ecs:UntagResource"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
            }
        }
    ]
}
```

> **Note**
>
> Ao usar tags de inclusão para seus clusters do Amazon ECS, você não precisa habilitar explicitamente o gerenciamento automático de GuardDuty agentes.

4. Quando você GuardDuty deseja monitorar tarefas que fazem parte de um serviço, é necessária a implantação de um novo serviço após a ativação do Runtime Monitoring. Se a última implantação de um serviço ECS específico foi iniciada antes de você habilitar o Monitoramento de runtime, você pode reiniciar o serviço ou atualizar o serviço usando `forceNewDeployment`.

   Nas etapas de atualização do serviço, consulte os seguintes recursos:

   - Atualização de um serviço Amazon ECS usando o console no Guia do desenvolvedor Amazon Elastic Container Service.
   - UpdateServicena Referência de API do Amazon Elastic Container Service.

- update-service na Referência de comando da AWS CLI .

Habilitação da configuração de agente automatizado para contas-membro ativas existentes

Manage for all Amazon ECS clusters (account level)

1. Na página Monitoramento de runtime, na guia Configuração, é possível visualizar o status atual da Configuração de agente automatizado.
2. No painel Configuração de agente automatizado, na seção Contas-membro ativas, escolha Ações.
3. Em Ações, escolha Habilitar para todas as contas-membro ativas existentes.
4. Escolha Confirmar.
5. Quando você GuardDuty deseja monitorar tarefas que fazem parte de um serviço, é necessária a implantação de um novo serviço após a ativação do Runtime Monitoring. Se a última implantação de um serviço ECS específico foi iniciada antes de você habilitar o Monitoramento de runtime, você pode reiniciar o serviço ou atualizar o serviço usando `forceNewDeployment`.

   Nas etapas de atualização do serviço, consulte os seguintes recursos:

   - Atualização de um serviço Amazon ECS usando o console no Guia do desenvolvedor Amazon Elastic Container Service.
   - UpdateServicena Referência de API do Amazon Elastic Container Service.
   - update-service na Referência de comando da AWS CLI .

Manage for all Amazon ECS clusters but exclude some of the clusters (cluster level)

1. Adicione uma tag a esse cluster do Amazon ECS com o par chave-valor como `GuardDutyManaged-false`.
2. Impeça a modificação de tags, exceto pelas entidades confiáveis. A política fornecida em Impedir que as tags sejam modificadas, exceto pelos princípios autorizados no Guia do usuário AWS Organizations foi modificada para ser aplicável aqui.

   JSON

```
{
```

```
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:TagResource",
                "ecs:UntagResource"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "ecs:ResourceTag/GuardDutyManaged":
 "${aws:PrincipalTag/GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "Null": {
                    "ecs:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:TagResource",
                "ecs:UntagResource"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/GuardDutyManaged":
 "${aws:PrincipalTag/GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyManaged"
```

```
                    ]
                }
            }
        },
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
            "Action": [
                "ecs:TagResource",
                "ecs:UntagResource"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
            }
        }
    ]
}
```

3. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.
4. No painel de navegação, escolha Monitoramento de runtime.
5.

> **Note**
>
> Sempre adicione a tag de exclusão aos seus clusters do Amazon ECS antes de ativar a configuração automática do agente para sua conta; caso contrário, o contêiner GuardDuty auxiliar será anexado a todos os contêineres nas tarefas do Amazon ECS que forem iniciadas.

   Na guia Configuração, na seção Configuração automatizada do agente, em Contas-membro ativas, escolha Ações.
6. Em Ações, escolha Habilitar para todas as contas-membro ativas.

Para os clusters do Amazon ECS que não foram excluídos, GuardDuty gerenciaremos a implantação do agente de segurança no contêiner auxiliar.

7. Escolha Confirmar.
8. Quando você GuardDuty deseja monitorar tarefas que fazem parte de um serviço, é necessária a implantação de um novo serviço após a ativação do Runtime Monitoring. Se a última implantação de um serviço ECS específico foi iniciada antes de você habilitar o Monitoramento de runtime, você pode reiniciar o serviço ou atualizar o serviço usando `forceNewDeployment`.

   Nas etapas de atualização do serviço, consulte os seguintes recursos:

   - Atualização de um serviço Amazon ECS usando o console no Guia do desenvolvedor Amazon Elastic Container Service.
   - UpdateServicena Referência de API do Amazon Elastic Container Service.
   - update-service na Referência de comando da AWS CLI .

Manage for selective (inclusion only) Amazon ECS clusters (cluster level)

1. Adicione uma tag a um cluster do Amazon ECS para o qual você deseja incluir todas as tarefas. O par chave-valor deve ser `GuardDutyManaged-true`.
2. Impeça a modificação dessas tags, exceto pelas entidades confiáveis. A política fornecida em Impedir que as tags sejam modificadas, exceto pelos princípios autorizados no Guia do usuário AWS Organizations foi modificada para ser aplicável aqui.

   JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:TagResource",
                "ecs:UntagResource"
            ],
            "Resource": [
```

```
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "ecs:ResourceTag/GuardDutyManaged":
 "${aws:PrincipalTag/GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "Null": {
                    "ecs:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:TagResource",
                "ecs:UntagResource"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/GuardDutyManaged":
 "${aws:PrincipalTag/GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyManaged"
                    ]
                }
            }
        },
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
            "Action": [
                "ecs:TagResource",
                "ecs:UntagResource"
```

```
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
            }
        }
    ]
}
```

> **Note**
>
> Ao usar tags de inclusão para seus clusters do Amazon ECS, não é preciso habilitar explicitamente a Configuração automatizada do agente.

3. Quando você GuardDuty deseja monitorar tarefas que fazem parte de um serviço, é necessária a implantação de um novo serviço após a ativação do Runtime Monitoring. Se a última implantação de um serviço ECS específico foi iniciada antes de você habilitar o Monitoramento de runtime, você pode reiniciar o serviço ou atualizar o serviço usando `forceNewDeployment`.

   Nas etapas de atualização do serviço, consulte os seguintes recursos:

   - Atualização de um serviço Amazon ECS usando o console no Guia do desenvolvedor Amazon Elastic Container Service.
   - UpdateServicena Referência de API do Amazon Elastic Container Service.
   - update-service na Referência de comando da AWS CLI .

Auto-enable Configuração automatizada de agentes para novos membros

Manage for all Amazon ECS clusters (account level)

1. Na página Monitoramento de runtime, escolha Editar para atualizar a configuração existente.
2. Na seção Configuração automatizada do agente, selecione Habilitar automaticamente para novas contas de membros.
3. Escolha Salvar.
4. Quando você GuardDuty deseja monitorar tarefas que fazem parte de um serviço, é necessária a implantação de um novo serviço após a ativação do Runtime Monitoring. Se a última implantação de um serviço ECS específico foi iniciada antes de você habilitar o Monitoramento de runtime, você pode reiniciar o serviço ou atualizar o serviço usando `forceNewDeployment`.

   Nas etapas de atualização do serviço, consulte os seguintes recursos:

   - Atualização de um serviço Amazon ECS usando o console no Guia do desenvolvedor Amazon Elastic Container Service.
   - UpdateServicena Referência de API do Amazon Elastic Container Service.
   - update-service na Referência de comando da AWS CLI .

Manage for all Amazon ECS clusters but exclude some of the clusters (cluster level)

1. Adicione uma tag a esse cluster do Amazon ECS com o par chave-valor como `GuardDutyManaged-false`.
2. Impeça a modificação de tags, exceto pelas entidades confiáveis. A política fornecida em Impedir que as tags sejam modificadas, exceto pelos princípios autorizados no Guia do usuário AWS Organizations foi modificada para ser aplicável aqui.

   JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
```

```
            "Action": [
                "ecs:TagResource",
                "ecs:UntagResource"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "ecs:ResourceTag/GuardDutyManaged":
 "${aws:PrincipalTag/GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "Null": {
                    "ecs:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:TagResource",
                "ecs:UntagResource"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/GuardDutyManaged":
 "${aws:PrincipalTag/GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyManaged"
                    ]
                }
            }
        },
        {
```

```
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
            "Action": [
                "ecs:TagResource",
                "ecs:UntagResource"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
            }
        }
    ]
}
```

3. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.
4. No painel de navegação, escolha Monitoramento de runtime.
5.

> **Note**
>
> Sempre adicione a tag de exclusão aos seus clusters do Amazon ECS antes de ativar a configuração automática do agente para sua conta; caso contrário, o contêiner GuardDuty auxiliar será anexado a todos os contêineres nas tarefas do Amazon ECS que forem iniciadas.

   Na guia Configuração, selecione Habilitar automaticamente para novas contas-membro na seção Configuração automatizada do agente.

   Para os clusters do Amazon ECS que não foram excluídos, GuardDuty gerenciaremos a implantação do agente de segurança no contêiner auxiliar.
6. Escolha Salvar.
7. Quando você GuardDuty deseja monitorar tarefas que fazem parte de um serviço, é necessária a implantação de um novo serviço após a ativação do Runtime Monitoring.

Se a última implantação de um serviço ECS específico foi iniciada antes de você habilitar o Monitoramento de runtime, você pode reiniciar o serviço ou atualizar o serviço usando `forceNewDeployment`.

Nas etapas de atualização do serviço, consulte os seguintes recursos:

- Atualização de um serviço Amazon ECS usando o console no Guia do desenvolvedor Amazon Elastic Container Service.
- UpdateServicena Referência de API do Amazon Elastic Container Service.
- update-service na Referência de comando da AWS CLI .

Manage for selective (inclusion only) Amazon ECS clusters (cluster level)

1. Adicione uma tag a um cluster do Amazon ECS para o qual você deseja incluir todas as tarefas. O par chave-valor deve ser `GuardDutyManaged-true`.
2. Impeça a modificação dessas tags, exceto pelas entidades confiáveis. A política fornecida em Impedir que as tags sejam modificadas, exceto pelos princípios autorizados no Guia do usuário AWS Organizations foi modificada para ser aplicável aqui.

   JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:TagResource",
                "ecs:UntagResource"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "ecs:ResourceTag/GuardDutyManaged":
 "${aws:PrincipalTag/GuardDutyManaged}",
```

```
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "Null": {
                    "ecs:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:TagResource",
                "ecs:UntagResource"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/GuardDutyManaged":
 "${aws:PrincipalTag/GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyManaged"
                    ]
                }
            }
        },
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
            "Action": [
                "ecs:TagResource",
                "ecs:UntagResource"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
```

```
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
            }
        }
    ]
}
```

> **Note**
>
> Ao usar tags de inclusão para seus clusters do Amazon ECS, não é preciso habilitar explicitamente a Configuração automatizada do agente.

3. Quando você GuardDuty deseja monitorar tarefas que fazem parte de um serviço, é necessária a implantação de um novo serviço após a ativação do Runtime Monitoring. Se a última implantação de um serviço ECS específico foi iniciada antes de você habilitar o Monitoramento de runtime, você pode reiniciar o serviço ou atualizar o serviço usando `forceNewDeployment`.

   Nas etapas de atualização do serviço, consulte os seguintes recursos:

   - Atualização de um serviço Amazon ECS usando o console no Guia do desenvolvedor Amazon Elastic Container Service.
   - UpdateServicena Referência de API do Amazon Elastic Container Service.
   - update-service na Referência de comando da AWS CLI .

Habilitando seletivamente a Configuração automatizada de agente para contas-membro ativas

Manage for all Amazon ECS (account level)

1. Na página Contas, selecione as contas para as quais você deseja ativar a configuração do Monitoring-Automated agente Runtime (ECS-Fargate). Você pode selecionar várias contas. Certifique-se de que as contas selecionadas nesta etapa já estejam habilitadas com Monitoramento de runtime.

2. Em Editar planos de proteção, escolha a opção apropriada para ativar a configuração do Monitoring-Automated agente Runtime (ECS-Fargate).
3. Escolha Confirmar.
4. Quando você GuardDuty deseja monitorar tarefas que fazem parte de um serviço, é necessária a implantação de um novo serviço após a ativação do Runtime Monitoring. Se a última implantação de um serviço ECS específico foi iniciada antes de você habilitar o Monitoramento de runtime, você pode reiniciar o serviço ou atualizar o serviço usando `forceNewDeployment`.

   Nas etapas de atualização do serviço, consulte os seguintes recursos:

   - Atualização de um serviço Amazon ECS usando o console no Guia do desenvolvedor Amazon Elastic Container Service.
   - UpdateServicena Referência de API do Amazon Elastic Container Service.
   - update-service na Referência de comando da AWS CLI .

Manage for all Amazon ECS clusters but exclude some of the clusters (cluster level)

1. Adicione uma tag a esse cluster do Amazon ECS com o par chave-valor como `GuardDutyManaged-false`.
2. Impeça a modificação de tags, exceto pelas entidades confiáveis. A política fornecida em Impedir que as tags sejam modificadas, exceto pelos princípios autorizados no Guia do usuário AWS Organizations foi modificada para ser aplicável aqui.

   JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:TagResource",
                "ecs:UntagResource"
            ],
            "Resource": [
                "*"
```

```
            ],
            "Condition": {
                "StringNotEquals": {
                    "ecs:ResourceTag/GuardDutyManaged":
 "${aws:PrincipalTag/GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "Null": {
                    "ecs:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:TagResource",
                "ecs:UntagResource"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/GuardDutyManaged":
 "${aws:PrincipalTag/GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyManaged"
                    ]
                }
            }
        },
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
            "Action": [
                "ecs:TagResource",
                "ecs:UntagResource"
            ],
```

```
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
            }
        }
    ]
}
```

3. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.
4. No painel de navegação, escolha Monitoramento de runtime.
5.

> **Note**
>
> Sempre adicione a tag de exclusão aos seus clusters do Amazon ECS antes de ativar o gerenciamento automático do GuardDuty agente para sua conta; caso contrário, o GuardDuty contêiner auxiliar será anexado a todos os contêineres nas tarefas do Amazon ECS que forem iniciadas.

   Na página Contas, selecione as contas para as quais você deseja ativar a configuração do Monitoring-Automated agente Runtime (ECS-Fargate). Você pode selecionar várias contas. Certifique-se de que as contas selecionadas nesta etapa já estejam habilitadas com Monitoramento de runtime.

   Para os clusters do Amazon ECS que não foram excluídos, GuardDuty gerenciaremos a implantação do agente de segurança no contêiner auxiliar.
6. Em Editar planos de proteção, escolha a opção apropriada para ativar a configuração do Monitoring-Automated agente Runtime (ECS-Fargate).
7. Escolha Salvar.
8. Quando você GuardDuty deseja monitorar tarefas que fazem parte de um serviço, é necessária a implantação de um novo serviço após a ativação do Runtime Monitoring. Se a última implantação de um serviço ECS específico foi iniciada antes de você habilitar

o Monitoramento de runtime, você pode reiniciar o serviço ou atualizar o serviço usando `forceNewDeployment`.

Nas etapas de atualização do serviço, consulte os seguintes recursos:

- Atualização de um serviço Amazon ECS usando o console no Guia do desenvolvedor Amazon Elastic Container Service.
- UpdateServicena Referência de API do Amazon Elastic Container Service.
- update-service na Referência de comando da AWS CLI .

Manage for selective (inclusion only) Amazon ECS clusters (cluster level)

1. Certifique-se de não habilitar a configuração automática do agente (ou a configuração do Monitoring-Automated agente Runtime (ECS-Fargate)) para as contas selecionadas que têm os clusters do Amazon ECS que você deseja monitorar.
2. Adicione uma tag a um cluster do Amazon ECS para o qual você deseja incluir todas as tarefas. O par chave-valor deve ser `GuardDutyManaged-true`.
3. Impeça a modificação dessas tags, exceto pelas entidades confiáveis. A política fornecida em Impedir que as tags sejam modificadas, exceto pelos princípios autorizados no Guia do usuário AWS Organizations foi modificada para ser aplicável aqui.

   JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:TagResource",
                "ecs:UntagResource"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
```

```
                    "ecs:ResourceTag/GuardDutyManaged":
 "${aws:PrincipalTag/GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "Null": {
                    "ecs:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:TagResource",
                "ecs:UntagResource"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/GuardDutyManaged":
 "${aws:PrincipalTag/GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyManaged"
                    ]
                }
            }
        },
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
            "Action": [
                "ecs:TagResource",
                "ecs:UntagResource"
            ],
            "Resource": [
                "*"
            ],
```

```
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
            }
        }
    ]
}
```

> **Note**
>
> Ao usar tags de inclusão para seus clusters do Amazon ECS, não é preciso habilitar explicitamente a Configuração automatizada do agente.

4. Quando você GuardDuty deseja monitorar tarefas que fazem parte de um serviço, é necessária a implantação de um novo serviço após a ativação do Runtime Monitoring. Se a última implantação de um serviço ECS específico foi iniciada antes de você habilitar o Monitoramento de runtime, você pode reiniciar o serviço ou atualizar o serviço usando `forceNewDeployment`.

   Nas etapas de atualização do serviço, consulte os seguintes recursos:

   - Atualização de um serviço Amazon ECS usando o console no Guia do desenvolvedor Amazon Elastic Container Service.
   - UpdateServicena Referência de API do Amazon Elastic Container Service.
   - update-service na Referência de comando da AWS CLI .

Configurando o GuardDuty agente para uma conta independente

1. Faça login no Console de gerenciamento da AWS e abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.
2. No painel de navegação, escolha Monitoramento de runtime.
3. Na guia Configuração:

a. Para gerenciar a Configuração automatizada de agente para todos os clusters do Amazon ECS (nível da conta)

   Selecione Habilitar na seção Configuração automatizada do agente para AWS Fargate (apenas ECS). Quando uma nova tarefa do Fargate Amazon ECS for iniciada, GuardDuty gerenciará a implantação do agente de segurança.

   - Escolha Salvar.

b. Para gerenciar a Configuração automatizada do agente excluindo alguns dos clusters do Amazon ECS (nível de cluster)

   i. Adicione uma tag a um cluster do Amazon ECS para o qual você deseja excluir todas as tarefas. O par chave-valor deve ser `GuardDutyManaged-false`.

   ii. Impeça a modificação dessas tags, exceto pelas entidades confiáveis. A política fornecida em Impedir que as tags sejam modificadas, exceto pelos princípios autorizados no Guia do usuário AWS Organizations foi modificada para ser aplicável aqui.

   JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:TagResource",
                "ecs:UntagResource"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "ecs:ResourceTag/GuardDutyManaged":
 "${aws:PrincipalTag/GuardDutyManaged}",
                    "aws:PrincipalArn":
 "arn:aws:iam::123456789012:role/org-admins/iam-admin"
```

```
                },
                "Null": {
                    "ecs:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:TagResource",
                "ecs:UntagResource"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/GuardDutyManaged":
"${aws:PrincipalTag/GuardDutyManaged}",
                    "aws:PrincipalArn":
"arn:aws:iam::123456789012:role/org-admins/iam-admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyManaged"
                    ]
                }
            }
        },
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
            "Action": [
                "ecs:TagResource",
                "ecs:UntagResource"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn":
"arn:aws:iam::123456789012:role/org-admins/iam-admin"
```

```
                },
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
            }
        }
    ]
}
```

iii. Na guia Configuração, escolha Habilitar na seção Configuração automatizada do agente.

> **Note**
>
> Sempre adicione a tag de exclusão ao seu cluster do Amazon ECS antes de ativar o gerenciamento automático do GuardDuty agente para sua conta; caso contrário, o agente de segurança será implantado em todas as tarefas que forem iniciadas no cluster correspondente do Amazon ECS.

Para os clusters do Amazon ECS que não foram excluídos, GuardDuty gerenciaremos a implantação do agente de segurança no contêiner auxiliar.

iv. Escolha Salvar.

c. Para gerenciar a Configuração automatizada de agente incluindo alguns dos clusters do Amazon ECS (nível de cluster)

i. Adicione uma tag a um cluster do Amazon ECS para o qual você deseja incluir todas as tarefas. O par chave-valor deve ser `GuardDutyManaged-true`.

ii. Impeça a modificação dessas tags, exceto pelas entidades confiáveis. A política fornecida em Impedir que as tags sejam modificadas, exceto pelos princípios autorizados no Guia do usuário AWS Organizations foi modificada para ser aplicável aqui.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
```

```
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:TagResource",
                "ecs:UntagResource"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "ecs:ResourceTag/GuardDutyManaged":
"${aws:PrincipalTag/GuardDutyManaged}",
                    "aws:PrincipalArn":
"arn:aws:iam::123456789012:role/org-admins/iam-admin"
                },
                "Null": {
                    "ecs:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:TagResource",
                "ecs:UntagResource"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/GuardDutyManaged":
"${aws:PrincipalTag/GuardDutyManaged}",
                    "aws:PrincipalArn":
"arn:aws:iam::123456789012:role/org-admins/iam-admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyManaged"
                    ]
                }
            }
```

```
        },
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
            "Action": [
                "ecs:TagResource",
                "ecs:UntagResource"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn":
 "arn:aws:iam::123456789012:role/org-admins/iam-admin"
                },
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
            }
        }
    ]
}
```

4. Quando você GuardDuty deseja monitorar tarefas que fazem parte de um serviço, é necessária a implantação de um novo serviço após a ativação do Runtime Monitoring. Se a última implantação de um serviço ECS específico foi iniciada antes de você habilitar o Monitoramento de runtime, você pode reiniciar o serviço ou atualizar o serviço usando `forceNewDeployment`.

   Nas etapas de atualização do serviço, consulte os seguintes recursos:

   - Atualização de um serviço Amazon ECS usando o console no Guia do desenvolvedor Amazon Elastic Container Service.
   - UpdateServicena Referência de API do Amazon Elastic Container Service.
   - update-service na Referência de comando da AWS CLI .

Gerenciando automaticamente o agente de segurança para recursos do Amazon EKS

O Runtime Monitoring suporta a ativação do agente de segurança por meio de configuração GuardDuty automática e manual. Esta seção fornece as etapas para habilitar a configuração de agente automatizado para clusters do Amazon EKS.

Antes de continuar, certifique-se de que você tenha seguido o Pré-requisitos para o suporte ao cluster do Amazon EKS.

Com base em sua abordagem preferida sobre como Configuração automatizada do agente (recomendada), escolha adequadamente as etapas nas seções a seguir.

Configuração de agente automatizado para ambiente de várias contas

Em ambientes de várias contas, somente a conta de GuardDuty administrador delegado pode ativar ou desativar a configuração automatizada do agente para as contas dos membros e gerenciar o agente automatizado para os clusters EKS pertencentes às contas dos membros em sua organização. As contas GuardDuty dos membros não podem modificar essa configuração em suas contas. A conta de GuardDuty administrador delegado gerencia suas contas de membros usando AWS Organizations. Para obter mais informações sobre ambientes com várias contas, consulte Gerenciar de várias contas.

Configurando a configuração automatizada do agente para a conta de administrador delegado GuardDuty

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
Gerencie o agente de segurança por meio de GuardDuty (Monitorar todos os clusters do EKS)	Se escolher Habilitar para todas as contas na seção Monitoramento de runtime, você terá as seguintes opções: • Escolha Ativar para todas as contas na seção Configuração automática do agente. GuardDuty implantará e gerenciará o agente de segurança para todos os clusters EKS que pertencem à conta de GuardDuty administrador delegada e também para todos os clusters EKS que pertencem a todas as contas membros existentes e potencialmente novas na organização.

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
	• Escolha Configurar contas manualmente. Se você escolheu Configurar contas manualmente na seção Monitoramento de runtime, faça o seguinte: 1. Selecione Configurar contas manualmente na seção Configuração de agente automatizado. 2. Escolha Habilitar na seção Conta de GuardDuty administrador delegado (esta conta). Escolha Salvar.

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
Monitorar todos os clusters do EKS, mas excluir alguns deles (usando tags de exclusão)	Nos procedimentos a seguir, escolha um dos cenários aplicáveis a você. Para excluir um cluster EKS do monitoramento quando o agente de GuardDuty segurança não foi implantado nesse cluster 1. Adicione uma tag a esse cluster do EKS com a chave como `GuardDutyManaged` e seu valor como `false`. Para obter mais informações sobre como marcar seu cluster do Amazon EKS, consulte Como trabalhar com tags usando o console no Guia do usuário do Amazon EKS. 2. Para evitar a modificação de tags, exceto pelas entidades confiáveis, use a política fornecida em Impedir que as tags sejam modificadas, exceto por diretores autorizados no Guia do usuário do AWS Organizations . Nessa política, substitua estes detalhes: • Substitua *ec2:CreateTags* por `eks:TagResource` . • Substitua *ec2:DeleteTags* por `eks:UntagResource` . • Substituir *access-project* por `GuardDutyManaged` • *123456789012* Substitua pelo Conta da AWS ID da entidade confiável. Quando você tiver mais de uma entidade confiável, use o exemplo a seguir para adicionar vários `PrincipalArn` : `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 3. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
	4. No painel de navegação, escolha Monitoramento de runtime. **Note** Sempre adicione a tag de exclusão aos seus clusters EKS antes de ativar o gerenciamento automático de GuardDuty agentes para sua conta; caso contrário, o agente de GuardDuty segurança será implantado em todos os clusters EKS em sua conta. 5. Na guia Configuração, escolha Habilitar na seção Gerenciam ento de GuardDuty agentes. Para os clusters EKS que não foram excluídos do monitoram ento, GuardDuty gerenciará a implantação e as atualizações do agente GuardDuty de segurança. 6. Escolha Salvar. Para excluir um cluster EKS do monitoramento quando o agente de GuardDuty segurança foi implantado nesse cluster 1. Adicione uma tag a esse cluster do EKS com a chave como `GuardDutyManaged` e seu valor como `false`. Para obter mais informações sobre como marcar seu cluster do Amazon EKS, consulte Como trabalhar com tags usando o console no Guia do usuário do Amazon EKS. 2. Para evitar a modificação de tags, exceto pelas entidades confiáveis, use a política fornecida em Impedir que as tags sejam modificadas, exceto por diretores autorizados no Guia do usuário do AWS Organizations . Nessa política, substitua estes detalhes: • Substitua *`ec2:CreateTags`* por `eks:TagResource` .

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
	• Substitua *ec2:DeleteTags* por `eks:UntagResource` . • Substituir *access-project* por `GuardDutyManaged` • *123456789012* Substitua pelo Conta da AWS ID da entidade confiável. Quando você tiver mais de uma entidade confiável, use o exemplo a seguir para adicionar vários `PrincipalArn` : `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 3. Se você tiver habilitado o agente automatizado para esse cluster EKS, depois dessa etapa, não GuardDuty atualizará o agente de segurança desse cluster. No entanto, o agente de segurança permanecerá implantado e GuardDuty continuará recebendo os eventos de tempo de execução desse cluster EKS. Isso pode afetar as estatísticas sobre seu uso. Para parar de receber os eventos de runtime desse cluster, você deve remover o agente de segurança implantado desse cluster do EKS. Para obter mais informações sobre a remoção do agente de segurança implantado, consulte Desativação, desinstalação e remoção de recursos no Monitoramento de runtime 4. Se você estava gerenciando o agente de GuardDuty segurança desse cluster EKS manualmente, consulteDesativação, desinstalação e remoção de recursos no Monitoramento de runtime.

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
Monitorar clusters do EKS seletivos usando tags de inclusão	Independentemente de como você escolheu habilitar o Monitoram ento de runtime, as etapas a seguir ajudarão você a monitorar clusters do EKS seletivos em sua conta: 1. Certifique-se de escolher Desativar para conta de GuardDuty administrador delegado (esta conta) na seção Configura ção automatizada do agente. Mantenha a configuração do Monitoramento de runtime igual à configurada na etapa anterior. 2. Escolha Salvar. 3. Adicione uma tag ao seu cluster do EKS com a chave como `GuardDutyManaged` e seu valor como `true`. Para obter mais informações sobre como marcar seu cluster do Amazon EKS, consulte Como trabalhar com tags usando o console no Guia do usuário do Amazon EKS. GuardDuty gerenciará a implantação e as atualizações do agente de segurança para os clusters EKS seletivos que você deseja monitorar. 4. Para evitar a modificação de tags, exceto pelas entidades confiáveis, use a política fornecida em Impedir que as tags sejam modificadas, exceto por diretores autorizados no Guia do usuário do AWS Organizations . Nessa política, substitua estes detalhes: • Substitua *`ec2:CreateTags`* por `eks:TagResource` . • Substitua *`ec2:DeleteTags`* por `eks:UntagResource` . • Substituir *`access-project`* por `GuardDutyManaged` • *`123456789012`* Substitua pelo Conta da AWS ID da entidade confiável. Quando você tiver mais de uma entidade confiável, use o exemplo a seguir para adicionar vários `PrincipalArn` :

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
	`"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]`
Gerencie o agente GuardDuty de segurança manualmente	Independentemente de como optou por habilitar o Monitoramento de runtime, é possível gerenciar o agente de segurança manualmente para seus clusters do EKS. 1. Certifique-se de escolher Desativar para conta de GuardDuty administrador delegado (esta conta) na seção Configuração automatizada do agente. Mantenha a configuração do Monitoramento de runtime igual à configurada na etapa anterior. 2. Escolha Salvar. 3. Para gerenciar o agente de segurança, consulte Como gerenciar o agente de segurança manualmente para o cluster Amazon EKS.

Auto-enable Agente automatizado para todas as contas de membros

> **Note**
>
> Pode levar até 24 horas para atualizar a configuração das contas-membro.

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
Gerencie o agente de segurança por meio de GuardDuty	Este tópico trata da habilitação do Monitoramento de runtime para todas as contas-membro e, portanto, as etapas a seguir pressupõem

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
(Monitorar todos os clusters do EKS)	que você deve ter escolhido Habilitar para todas as contas na seção Monitoramento de runtime. 1. Escolha Ativar para todas as contas na seção Configuração automática do agente. GuardDuty implantará e gerenciará o agente de segurança para todos os clusters EKS que pertencem à conta de GuardDuty administrador delegada e também para todos os clusters EKS que pertencem a todas as contas membros existentes e potencialmente novas na organização. 2. Escolha Salvar.

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
Monitorar todos os clusters do EKS, mas excluir alguns deles (usando tags de exclusão)	Nos procedimentos a seguir, escolha um dos cenários aplicáveis a você. Para excluir um cluster EKS do monitoramento quando o agente de GuardDuty segurança não foi implantado nesse cluster 1. Adicione uma tag a esse cluster do EKS com a chave como `GuardDutyManaged` e seu valor como `false`. Para obter mais informações sobre como marcar seu cluster do Amazon EKS, consulte Como trabalhar com tags usando o console no Guia do usuário do Amazon EKS. 2. Para evitar a modificação de tags, exceto pelas entidades confiáveis, use a política fornecida em Impedir que as tags sejam modificadas, exceto por diretores autorizados no Guia do usuário do AWS Organizations . Nessa política, substitua estes detalhes: • Substitua *`ec2:CreateTags`* por `eks:TagResource` . • Substitua *`ec2:DeleteTags`* por `eks:UntagResource` . • Substituir *`access-project`* por `GuardDutyManaged` • *`123456789012`* Substitua pelo Conta da AWS ID da entidade confiável. Quando você tiver mais de uma entidade confiável, use o exemplo a seguir para adicionar vários `PrincipalArn` : `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 3. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
	4. No painel de navegação, escolha Monitoramento de runtime. **Note** Sempre adicione a tag de exclusão aos seus clusters EKS antes de ativar o agente automatizado para sua conta; caso contrário, o agente de GuardDuty segurança será implantado em todos os clusters EKS em sua conta. 5. Na guia Configuração, escolha Editar na seção Configuração do Monitoramento de runtime. 6. Selecione Habilitar para todas as contas na seção Configuração automatizada do agente. Para os clusters EKS que não foram excluídos do monitoramento, GuardDuty gerenciará a implantaç ão e as atualizações do agente GuardDuty de segurança. 7. Escolha Salvar. Para excluir um cluster EKS do monitoramento quando o agente de GuardDuty segurança foi implantado nesse cluster 1. Adicione uma tag a esse cluster do EKS com a chave como `GuardDutyManaged` e seu valor como `false`. Para obter mais informações sobre como marcar seu cluster do Amazon EKS, consulte Como trabalhar com tags usando o console no Guia do usuário do Amazon EKS. 2. Se você tiver a configuração automatizada do agente habilitad a para esse cluster EKS, depois dessa etapa, não GuardDuty atualizará o agente de segurança desse cluster. No entanto, o agente de segurança permanecerá implantado e GuardDuty continuará recebendo os eventos de tempo de execução desse cluster EKS. Isso pode afetar as estatísticas sobre seu uso.

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
	Para parar de receber os eventos de runtime desse cluster, você deve remover o agente de segurança implantado desse cluster do EKS. Para obter mais informações sobre a remoção do agente de segurança implantado, consulte Desativação, desinstalação e remoção de recursos no Monitoramento de runtime 3. Para evitar a modificação de tags, exceto pelas entidades confiáveis, use a política fornecida em Impedir que as tags sejam modificadas, exceto por diretores autorizados no Guia do usuário do AWS Organizations . Nessa política, substitua estes detalhes: • Substitua *ec2:CreateTags* por `eks:TagResource` . • Substitua *ec2:DeleteTags* por `eks:UntagResource` . • Substituir *access-project* por `GuardDutyManaged` • *123456789012* Substitua pelo Conta da AWS ID da entidade confiável. Quando você tiver mais de uma entidade confiável, use o exemplo a seguir para adicionar vários `PrincipalArn` : `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 4. Se você estava gerenciando o agente de GuardDuty segurança desse cluster EKS manualmente, consulteDesativação, desinstalação e remoção de recursos no Monitoramento de runtime.

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
Monitorar clusters do EKS seletivos usando tags de inclusão	Independentemente de como você escolheu habilitar o Monitoram ento de runtime, as etapas a seguir ajudarão você a monitorar clusters do EKS seletivos para todas as contas-membro em sua organização: 1. Não habilite nenhuma configuração na seção Configuração de agente automatizado Mantenha a configuração do Monitoram ento de runtime igual à configurada na etapa anterior. 2. Escolha Salvar. 3. Adicione uma tag ao seu cluster do EKS com a chave como `GuardDutyManaged` e seu valor como `true`. Para obter mais informações sobre como marcar seu cluster do Amazon EKS, consulte Como trabalhar com tags usando o console no Guia do usuário do Amazon EKS. GuardDuty gerenciará a implantação e as atualizações do agente de segurança para os clusters EKS seletivos que você deseja monitorar. 4. Para evitar a modificação de tags, exceto pelas entidades confiáveis, use a política fornecida em Impedir que as tags sejam modificadas, exceto por diretores autorizados no Guia do usuário do AWS Organizations . Nessa política, substitua estes detalhes: • Substitua *`ec2:CreateTags`* por `eks:TagResource` . • Substitua *`ec2:DeleteTags`* por `eks:UntagResource` . • Substituir *`access-project`* por `GuardDutyManaged` • *`123456789012`* Substitua pelo Conta da AWS ID da entidade confiável. Quando você tiver mais de uma entidade confiável, use o exemplo a seguir para adicionar vários `PrincipalArn` :

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
	`"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]`
Gerencie o agente GuardDuty de segurança manualmente	Independentemente de como tenha optado por habilitar o Monitoramento de runtime, é possível gerenciar o agente de segurança manualmente para seus clusters do EKS. 1. Não habilite nenhuma configuração na seção Configuração de agente automatizado Mantenha a configuração do Monitoramento de runtime igual à configurada na etapa anterior. 2. Escolha Salvar. 3. Para gerenciar o agente de segurança, consulte Como gerenciar o agente de segurança manualmente para o cluster Amazon EKS.

Habilitando o agente automatizado para todas as contas de membros ativas existentes

> **Note**
>
> Pode levar até 24 horas para atualizar a configuração das contas-membro.

Para gerenciar o agente GuardDuty de segurança para contas de membros ativos existentes em sua organização

- GuardDuty Para receber os eventos de tempo de execução dos clusters EKS que pertencem às contas de membros ativos existentes na organização, você deve escolher uma abordagem preferida para gerenciar o agente de GuardDuty segurança desses clusters EKS. Para obter mais informações sobre essas abordagens, consulte Implantação do agente de segurança no Amazon EKS.

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
Gerencie o agente de segurança por meio de GuardDuty (Monitorar todos os clusters do EKS)	Para monitorar todos os clusters do EKS para todas as contas-membro ativas existentes 1. Na página Monitoramento de runtime, na guia Configuração, é possível visualizar o status atual da Configuração de agente automatizado. 2. No painel Configuração de agente automatizado, na seção Contas de membros ativas, selecione Ações. 3. Em Ações, escolha Habilitar para todas as contas-membro ativas existentes. 4. Escolha Confirmar.

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
Monitorar todos os clusters do EKS, mas excluir alguns deles (usando a tag de exclusão)	Nos procedimentos a seguir, escolha um dos cenários aplicáveis a você. Para excluir um cluster EKS do monitoramento quando o agente de GuardDuty segurança não foi implantado nesse cluster 1. Adicione uma tag a esse cluster do EKS com a chave como `GuardDutyManaged` e seu valor como `false`. Para obter mais informações sobre como marcar seu cluster do Amazon EKS, consulte Como trabalhar com tags usando o console no Guia do usuário do Amazon EKS. 2. Para evitar a modificação de tags, exceto pelas entidades confiáveis, use a política fornecida em Impedir que as tags sejam modificadas, exceto por diretores autorizados no Guia do usuário do AWS Organizations . Nessa política, substitua estes detalhes: • Substitua *`ec2:CreateTags`* por `eks:TagResource` . • Substitua *`ec2:DeleteTags`* por `eks:UntagResource` . • Substituir *`access-project`* por `GuardDutyManaged` • *`123456789012`* Substitua pelo Conta da AWS ID da entidade confiável.

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
	Quando você tiver mais de uma entidade confiável, use o exemplo a seguir para adicionar vários `PrincipalArn` : `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 3. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/. 4. No painel de navegação, escolha Monitoramento de runtime. **Note** Sempre adicione a tag de exclusão aos seus clusters EKS antes de ativar a configuração automática do agente para sua conta; caso contrário, o agente de GuardDuty segurança será implantado em todos os clusters EKS em sua conta. 5. Na guia Configuração, no painel Configuração de agente automatizado, em Contas de membros ativas, selecione Ações. 6. Em Ações, escolha Habilitar para todas as contas-membro ativas. 7. Escolha Confirmar.

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
	Para excluir um cluster EKS do monitoramento após o agente GuardDuty de segurança já ter sido implantado nesse cluster 1. Adicione uma tag a esse cluster do EKS com a chave como `GuardDutyManaged` e seu valor como `false`. Para obter mais informações sobre como marcar seu cluster do Amazon EKS, consulte Como trabalhar com tags usando o console no Guia do usuário do Amazon EKS. Após essa etapa, não GuardDuty atualizará o agente de segurança desse cluster. No entanto, o agente de segurança permanecerá implantado e GuardDuty continuará recebendo os eventos de tempo de execução desse cluster EKS. Isso pode afetar as estatísticas sobre seu uso. 2. Para evitar a modificação de tags, exceto pelas entidades confiáveis, use a política fornecida em Impedir que as tags sejam modificadas, exceto por diretores autorizados no Guia do usuário do AWS Organizations . Nessa política, substitua estes detalhes: • Substitua *`ec2:CreateTags`* por `eks:TagResource` . • Substitua *`ec2:DeleteTags`* por `eks:UntagResource` . • Substituir *`access-project`* por `GuardDutyManaged`

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
	• *123456789012* Substitua pelo Conta da AWS ID da entidade confiável. Quando você tiver mais de uma entidade confiável, use o exemplo a seguir para adicionar vários `PrincipalArn` : `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 3. Independentemente de como você gerencia o agente de segurança (por meio GuardDuty ou manualmente), para parar de receber os eventos de tempo de execução desse cluster, você deve remover o agente de segurança implantado desse cluster EKS. Para obter mais informações sobre a remoção do agente de segurança implantado, consulte Desativação, desinstalação e remoção de recursos no Monitoramento de runtime.

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
Monitorar clusters do EKS seletivos usando tags de inclusão	1. Na página Contas, depois de ativar o Monitoramento de runtime, não habilite Monitoramento de runtime - Configuração de agente automatizado. 2. Adicione uma tag ao cluster do EKS que pertence à conta selecionada que você deseja monitorar. O par de chave-valor da tag deve ser `GuardDuty Managed -true`. Para obter mais informações sobre como marcar seu cluster do Amazon EKS, consulte Como trabalhar com tags usando o console no Guia do usuário do Amazon EKS. GuardDuty gerenciará a implantação e as atualizaç ões do agente de segurança para os clusters EKS seletivos que você deseja monitorar. 3. Para evitar a modificação de tags, exceto pelas entidades confiáveis, use a política fornecida em Impedir que as tags sejam modificadas, exceto por diretores autorizados no Guia do usuário do AWS Organizations . Nessa política, substitua estes detalhes: • Substitua *`ec2:CreateTags`* por `eks:TagRe source` . • Substitua *`ec2:DeleteTags`* por `eks:Untag Resource` . • Substituir *`access-project`* por `GuardDuty Managed` • *`123456789012`* Substitua pelo Conta da AWS ID da entidade confiável.

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
	Quando você tiver mais de uma entidade confiável, use o exemplo a seguir para adicionar vários `PrincipalArn` : `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]`
Gerencie o agente GuardDuty de segurança manualmente	1. Certifique-se de não selecionar Habilitar na seção Configuração de agente automatizado. Mantenha o Monitoramento de runtime habilitado. 2. Escolha Salvar. 3. Para gerenciar o agente de segurança, consulte Como gerenciar o agente de segurança manualmente para o cluster Amazon EKS.

Auto-enable configuração automatizada de agentes para novos membros

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
Gerencie o agente de segurança por meio de GuardDuty (Monitorar todos os clusters do EKS)	1. Na página Monitoramento de runtime, escolha Editar para atualizar a configuração existente. 2. Na seção Configuração automatizada do agente, selecione Habilitar automaticamente para novas contas de membros. 3. Escolha Salvar.

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
Monitorar todos os clusters do EKS, mas excluir alguns deles (usando tags de exclusão)	Nos procedimentos a seguir, escolha um dos cenários aplicáveis a você. Para excluir um cluster EKS do monitoramento quando o agente de GuardDuty segurança não foi implantado nesse cluster 1. Adicione uma tag a esse cluster do EKS com a chave como `GuardDutyManaged` e seu valor como `false`. Para obter mais informações sobre como marcar seu cluster do Amazon EKS, consulte Como trabalhar com tags usando o console no Guia do usuário do Amazon EKS. 2. Para evitar a modificação de tags, exceto pelas entidades confiáveis, use a política fornecida em Impedir que as tags sejam modificadas, exceto por diretores autorizados no Guia do usuário do AWS Organizations . Nessa política, substitua estes detalhes: • Substitua *`ec2:CreateTags`* por `eks:TagResource` . • Substitua *`ec2:DeleteTags`* por `eks:UntagResource` . • Substituir *`access-project`* por `GuardDutyManaged` • *`123456789012`* Substitua pelo Conta da AWS ID da entidade confiável. Quando você tiver mais de uma entidade confiável , use o exemplo a seguir para adicionar vários `PrincipalArn` :

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas

```
"aws:PrincipalArn":["arn:aws:iam::12
3456789012:role/org-admins/iam-admin
", "arn:aws:iam::123456789012:role/org-
admins/iam-admin", "arn:aws:iam::1234
56789012:role/org-admins/iam-admin"]
```

3. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.
4. No painel de navegação, escolha Monitoramento de runtime.

> **Note**
>
> Sempre adicione a tag de exclusão aos seus clusters EKS antes de ativar a configuração automática do agente para sua conta; caso contrário, o agente de GuardDuty segurança será implantado em todos os clusters EKS em sua conta.

5. Na guia Configuração, selecione Ativar automaticamente para novas contas de membros na seção de gerenciamento de GuardDuty agentes.

   Para os clusters EKS que não foram excluídos do monitoramento, GuardDuty gerenciará a implantação e as atualizações do agente GuardDuty de segurança.
6. Escolha Salvar.

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
	Para excluir um cluster EKS do monitoramento quando o agente de GuardDuty segurança foi implantado nesse cluster 1. Independentemente de você gerenciar o agente GuardDuty de segurança por meio GuardDuty ou manualmente, adicione uma tag a esse cluster EKS com a chave como `GuardDutyManaged` e seu valor como`false`. Para obter mais informações sobre como marcar seu cluster do Amazon EKS, consulte Como trabalhar com tags usando o console no Guia do usuário do Amazon EKS. Se você tiver habilitado o agente automatizado para esse cluster EKS, depois dessa etapa, não GuardDuty atualizará o agente de segurança desse cluster. No entanto, o agente de segurança permanecerá implantado e GuardDuty continuará recebendo os eventos de tempo de execução desse cluster EKS. Isso pode afetar as estatísticas sobre seu uso. Para parar de receber os eventos de runtime desse cluster, você deve remover o agente de segurança implantado desse cluster do EKS. Para obter mais informações sobre a remoção do agente de segurança implantado, consulte Desativação, desinstalação e remoção de recursos no Monitoramento de runtime 2. Para evitar a modificação de tags, exceto pelas entidades confiáveis, use a política fornecida em Impedir que as tags sejam modificadas, exceto por diretores autorizados no Guia do usuário do AWS Organizations . Nessa política, substitua estes detalhes:

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
	• Substitua *ec2:CreateTags* por `eks:TagResource` . • Substitua *ec2:DeleteTags* por `eks:UntagResource` . • Substituir *access-project* por `GuardDutyManaged` • *123456789012* Substitua pelo Conta da AWS ID da entidade confiável. Quando você tiver mais de uma entidade confiável , use o exemplo a seguir para adicionar vários `PrincipalArn` : `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 3. Se você estava gerenciando o agente de GuardDuty segurança desse cluster EKS manualmente, consulteDesativação, desinstalação e remoção de recursos no Monitoramento de runtime.

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
Monitorar clusters do EKS seletivos usando tags de inclusão	Independentemente de como você escolheu habilitar o Monitoramento de runtime, as etapas a seguir ajudarão a monitorar clusters do EKS seletivos para as novas contas-membro em sua organização. 1. Certifique-se de desmarcar a opção Habilitar automatic amente para novas contas de membros na seção Configuração de agente automatizado. Mantenha a configuração do Monitoramento de runtime igual à configurada na etapa anterior. 2. Escolha Salvar. 3. Adicione uma tag ao seu cluster do EKS com a chave como `GuardDutyManaged` e seu valor como `true`. Para obter mais informações sobre como marcar seu cluster do Amazon EKS, consulte Como trabalhar com tags usando o console no Guia do usuário do Amazon EKS. GuardDuty gerenciará a implantação e as atualizações do agente de segurança para os clusters EKS seletivos que você deseja monitorar. 4. Para evitar a modificação de tags, exceto pelas entidades confiáveis, use a política fornecida em Impedir que as tags sejam modificadas, exceto por diretores autorizados no Guia do usuário do AWS Organizations . Nessa política, substitua estes detalhes: • Substitua *`ec2:CreateTags`* por `eks:TagResource` . • Substitua *`ec2:DeleteTags`* por `eks:UntagResource` .

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
	• Substituir *access-project* por `GuardDuty Managed` • *123456789012* Substitua pelo Conta da AWS ID da entidade confiável. Quando você tiver mais de uma entidade confiável, use o exemplo a seguir para adicionar vários `PrincipalArn` : `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]`
Gerencie o agente GuardDuty de segurança manualmente	Independentemente de como optou por habilitar o Monitoramento de runtime, é possível gerenciar o agente de segurança manualmente para seus clusters do EKS. 1. Certifique-se de desmarcar a caixa de seleção Habilitar automaticamente para novas contas de membros na seção Configuração de agente automatizado. Mantenha a configuração do Monitoramento de runtime igual à configurada na etapa anterior. 2. Escolha Salvar. 3. Para gerenciar o agente de segurança, consulte Como gerenciar o agente de segurança manualmente para o cluster Amazon EKS.

Configurando seletivamente o agente automatizado para contas-membro ativas

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
Gerencie o agente de segurança por meio de GuardDuty (Monitorar todos os clusters do EKS)	1. Na página Contas, selecione as contas para as quais deseja habilitar a opção Configuração de agente automatizado. É possível selecionar mais de uma conta por vez. Certifique-se de que as contas selecionadas nesta etapa já tenham o Monitoram ento de runtime do EKS habilitado. 2. Em Editar planos de proteção, selecione a opção apropriada para habilitar o Monitoramento de runtime - Configuração de agente automatizado. 3. Escolha Confirmar.
Monitorar todos os clusters do EKS, mas excluir alguns deles (usando tags de exclusão)	Nos procedimentos a seguir, escolha um dos cenários aplicáveis a você. Para excluir um cluster EKS do monitoramento quando o agente de GuardDuty segurança não foi implantado nesse cluster 1. Adicione uma tag a esse cluster do EKS com a chave como `GuardDutyManaged` e seu valor como `false`. Para obter mais informações sobre como marcar seu cluster do Amazon EKS, consulte Como trabalhar com tags usando o console no Guia do usuário do Amazon EKS. 2. Para evitar a modificação de tags, exceto pelas entidades confiáveis, use a política fornecida em Impedir que as tags sejam modificadas, exceto por diretores autorizados no Guia do usuário do AWS Organizations . Nessa política, substitua estes detalhes: • Substitua *`ec2:CreateTags`* por `eks:TagResource` . • Substitua *`ec2:DeleteTags`* por `eks:UntagResource` . • Substituir *`access-project`* por `GuardDutyManaged`

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas

- *123456789012* Substitua pelo Conta da AWS ID da entidade confiável.

  Quando você tiver mais de uma entidade confiável, use o exemplo a seguir para adicionar vários `PrincipalArn` :

  ```
  "aws:PrincipalArn":["arn:aws:iam::12345678901
  2:role/org-admins/iam-admin", "arn:aws:iam::1234
  56789012:role/org-admins/iam-admin", "arn:aws:
  iam::123456789012:role/org-admins/iam-admin"]
  ```

3. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.

   > **Note**
   >
   > Sempre adicione a tag de exclusão aos seus clusters EKS antes de ativar a configuração automática do agente para sua conta; caso contrário, o agente de GuardDuty segurança será implantado em todos os clusters EKS em sua conta.

4. Na página Contas, selecione a conta para a qual você deseja habilitar a opção Gerenciar o agente automaticamente. É possível selecionar mais de uma conta por vez.
5. Em Editar planos de proteção, escolha a opção apropriada para ativar a configuração do Monitoring-Automated agente Runtime para a conta selecionada.

   Para os clusters EKS que não foram excluídos do monitoram ento, GuardDuty gerenciará a implantação e as atualizações do agente GuardDuty de segurança.
6. Escolha Salvar.

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
	Para excluir um cluster EKS do monitoramento quando o agente de GuardDuty segurança foi implantado nesse cluster 1. Adicione uma tag a esse cluster do EKS com a chave como `GuardDutyManaged` e seu valor como `false`. Para obter mais informações sobre como marcar seu cluster do Amazon EKS, consulte Como trabalhar com tags usando o console no Guia do usuário do Amazon EKS. Se você já tinha a configuração automatizada do agente habilitada para esse cluster EKS, depois dessa etapa, não GuardDuty atualizará o agente de segurança desse cluster. No entanto, o agente de segurança permanecerá implantado e GuardDuty continuará recebendo os eventos de tempo de execução desse cluster EKS. Isso pode afetar as estatísticas sobre seu uso. Para parar de receber os eventos de runtime desse cluster, você deve remover o agente de segurança implantado desse cluster do EKS. Para obter mais informações sobre a remoção do agente de segurança implantado, consulte Desativação, desinstalação e remoção de recursos no Monitoramento de runtime 2. Para evitar a modificação de tags, exceto pelas entidades confiáveis, use a política fornecida em Impedir que as tags sejam modificadas, exceto por diretores autorizados no Guia do usuário do AWS Organizations . Nessa política, substitua estes detalhes: • Substitua *`ec2:CreateTags`* por `eks:TagResource` . • Substitua *`ec2:DeleteTags`* por `eks:UntagResource` . • Substituir *`access-project`* por `GuardDutyManaged`

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
	• *123456789012* Substitua pelo Conta da AWS ID da entidade confiável. Quando você tiver mais de uma entidade confiável, use o exemplo a seguir para adicionar vários `PrincipalArn` : `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 3. Se você estava gerenciando o agente de GuardDuty segurança desse cluster EKS manualmente, você deve removê-lo. Para obter mais informações, consulte Desativação, desinstalação e remoção de recursos no Monitoramento de runtime.

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
Monitorar clusters do EKS seletivos usando tags de inclusão	Independentemente de como você escolheu habilitar o Monitoram ento de runtime, as etapas a seguir ajudarão a monitorar clusters do EKS seletivos que pertencem às contas selecionadas: 1. Certifique-se de não habilitar a configuração do Monitoring-Automated agente Runtime para as contas selecionadas que têm os clusters EKS que você deseja monitorar. 2. Adicione uma tag ao seu cluster do EKS com a chave como `GuardDutyManaged` e seu valor como `true`. Para obter mais informações sobre como marcar seu cluster do Amazon EKS, consulte Como trabalhar com tags usando o console no Guia do usuário do Amazon EKS. Depois de adicionar a tag, GuardDuty gerenciará a implantação e as atualizações do agente de segurança para os clusters EKS seletivos que você deseja monitorar. 3. Para evitar a modificação de tags, exceto pelas entidades confiáveis, use a política fornecida em Impedir que as tags sejam modificadas, exceto por diretores autorizados no Guia do usuário do AWS Organizations . Nessa política, substitua estes detalhes: • Substitua *`ec2:CreateTags`* por `eks:TagResource` . • Substitua *`ec2:DeleteTags`* por `eks:UntagResource` . • Substituir *`access-project`* por `GuardDutyManaged` • *`123456789012`* Substitua pelo Conta da AWS ID da entidade confiável. Quando você tiver mais de uma entidade confiável, use o exemplo a seguir para adicionar vários `PrincipalArn` :

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
	`"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]`
Gerencie o agente GuardDuty de segurança manualmente	1. Mantenha a configuração do Monitoramento de runtime igual à configurada na etapa anterior. Certifique-se de não habilitar o Monitoramento de runtime - Configuração do agente automatizado para nenhuma das contas selecionadas. 2. Escolha Confirmar. 3. Para gerenciar o agente de segurança, consulte Como gerenciar o agente de segurança manualmente para o cluster Amazon EKS.

Configuração de agente automatizado para conta autônoma

Uma conta autônoma é responsável pela decisão de ativar ou desativar um plano de proteção Conta da AWS em uma conta específica Região da AWS.

Se sua conta estiver associada a uma conta de GuardDuty administrador por meio AWS Organizations ou pelo método de convite, esta seção não se aplica à sua conta. Para obter mais informações, consulte Habilitando o Monitoramento de runtime do EKS para ambientes com várias contas.

Depois de ativar o Runtime Monitoring, certifique-se de instalar o agente GuardDuty de segurança por meio de configuração automatizada ou implantação manual. Como parte da conclusão de todas as etapas listadas no procedimento a seguir, certifique-se de instalar o agente de segurança.

Com base em sua prioridade de monitorar todos os recursos do Amazon EKS ou recursos seletivos, escolha um método de acordo com sua preferência e siga as etapas da tabela a seguir.

1. Faça login no Console de gerenciamento da AWS e abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.

2. No painel de navegação, escolha Monitoramento de runtime.
3. Na guia Configuração, selecione Habilitar para habilitar a configuração de agente automático para sua conta.

Abordagem preferida para implantar o agente GuardDuty de segurança	Etapas
Gerencie o agente de segurança por meio de GuardDuty (Monitorar todos os clusters do EKS)	1. Escolha Ativar na seção Configuração automatizada do agente. GuardDuty gerenciará a implantação e as atualizações do agente de segurança para todos os clusters EKS existentes e potencialmente novos em sua conta. 2. Escolha Salvar.
Monitorar todos os clusters do EKS, mas excluir alguns deles (usando a tag de exclusão)	Nos procedimentos a seguir, escolha um dos cenários que se aplica a você. Para excluir um cluster EKS do monitoramento quando o agente de GuardDuty segurança não foi implantado nesse cluster 1. Adicione uma tag a esse cluster do EKS com a chave como `GuardDutyManaged` e seu valor como `false`. Para obter mais informações sobre como marcar seu cluster do Amazon EKS, consulte Como trabalhar com tags usando o console no Guia do usuário do Amazon EKS. 2. Para evitar a modificação de tags, exceto pelas entidades confiáveis, use a política fornecida em Impedir que as tags sejam modificadas, exceto por diretores autorizados no Guia do usuário do AWS Organizations . Nessa política, substitua estes detalhes:

Abordagem preferida para implantar o agente GuardDuty de segurança	Etapas
	• Substitua *ec2:CreateTags* por `eks:TagResource`. • Substitua *ec2:DeleteTags* por `eks:UntagResource`. • Substituir *access-project* por `GuardDutyManaged` • *123456789012* Substitua pelo Conta da AWS ID da entidade confiável. Quando você tiver mais de uma entidade confiável, use o exemplo a seguir para adicionar vários `PrincipalArn` : `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 3. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/. 4. No painel de navegação, escolha Monitoramento de runtime. **Note** Sempre adicione a tag de exclusão aos seus clusters EKS antes de ativar o gerenciamento automático de GuardDuty agentes para sua conta; caso contrário, o agente de GuardDuty segurança será implantado em todos os clusters EKS em sua conta.

Abordagem preferida para implantar o agente GuardDuty de segurança	Etapas
	5. Na guia Configuração, escolha Habilitar na seção Gerenciamento de GuardDuty agentes. Para os clusters EKS que não foram excluídos do monitoramento, GuardDuty gerenciará a implantação e as atualizações do agente GuardDuty de segurança. 6. Escolha Salvar. Para excluir um cluster EKS do monitoramento após o agente GuardDuty de segurança já ter sido implantado nesse cluster 1. Adicione uma tag a esse cluster do EKS com a chave como `GuardDutyManaged` e seu valor como `false`. Para obter mais informações sobre como marcar seu cluster do Amazon EKS, consulte Como trabalhar com tags usando o console no Guia do usuário do Amazon EKS. Após essa etapa, não GuardDuty atualizará o agente de segurança desse cluster. No entanto, o agente de segurança permanecerá implantado e GuardDuty continuará recebendo os eventos de tempo de execução desse cluster EKS. Isso pode afetar as estatísticas sobre seu uso. 2. Para evitar a modificação de tags, exceto pelas entidades confiáveis, use a política fornecida em Impedir que as tags sejam modificadas, exceto por diretores autorizados no Guia do usuário do

Abordagem preferida para implantar o agente GuardDuty de segurança	Etapas
	AWS Organizations . Nessa política, substitua estes detalhes: • Substitua *ec2:CreateTags* por `eks:TagResource` . • Substitua *ec2:DeleteTags* por `eks:UntagResource` . • Substituir *access-project* por `GuardDutyManaged` • *123456789012* Substitua pelo Conta da AWS ID da entidade confiável. Quando você tiver mais de uma entidade confiável , use o exemplo a seguir para adicionar vários `PrincipalArn` : `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 3. Para parar de receber os eventos de runtime desse cluster, você deve remover o agente de segurança implantado desse cluster do EKS. Para obter mais informações sobre a remoção do agente de segurança implantado, consulte Desativação, desinstalação e remoção de recursos no Monitoramento de runtime.

Abordagem preferida para implantar o agente GuardDuty de segurança	Etapas
Monitorar clusters do EKS seletivos usando tags de inclusão	1. Certifique-se de selecionar Desabilitar na seção Configuração de agente automatizado. Mantenha o Monitoramento de runtime habilitado. 2. Escolha Salvar 3. Adicione uma tag a esse cluster do EKS com a chave como `GuardDutyManaged` e seu valor como `true`. Para obter mais informações sobre como marcar seu cluster do Amazon EKS, consulte Como trabalhar com tags usando o console no Guia do usuário do Amazon EKS. GuardDuty gerenciará a implantação e as atualizaç ões do agente de segurança para os clusters EKS seletivos que você deseja monitorar. 4. Para evitar a modificação de tags, exceto pelas entidades confiáveis, use a política fornecida em Impedir que as tags sejam modificadas, exceto por diretores autorizados no Guia do usuário do AWS Organizations . Nessa política, substitua estes detalhes: • Substitua *ec2:CreateTags* por `eks:TagRe source` . • Substitua *ec2:DeleteTags* por `eks:Untag Resource` . • Substituir *access-project* por `GuardDuty Managed` • *123456789012* Substitua pelo Conta da AWS ID da entidade confiável.

Abordagem preferida para implantar o agente GuardDuty de segurança	Etapas
	Quando você tiver mais de uma entidade confiável, use o exemplo a seguir para adicionar vários `PrincipalArn` : `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]`
Gerenciar agente manualmente	1. Certifique-se de selecionar Desabilitar na seção Configuração de agente automatizado. Mantenha o Monitoramento de runtime habilitado. 2. Escolha Salvar. 3. Para gerenciar o agente de segurança, consulte Como gerenciar o agente de segurança manualmente para o cluster Amazon EKS.

Como gerenciar o agente de segurança manualmente para o cluster Amazon EKS

Esta seção descreve como você pode gerenciar seu agente complementar (GuardDuty agente) do Amazon EKS depois de ativar o Runtime Monitoring (ou EKS Runtime Monitoring). Para usar o Monitoramento de runtime, você deve habilitar o Monitoramento de runtime e configurar o complemento do Amazon EKS, `aws-guardduty-agent`. Você precisa executar as duas etapas GuardDuty para detectar e gerar ameaças em potencialGuardDuty Tipos de descoberta de monitoramento de tempo de execução.

Para gerenciar o agente manualmente, é preciso criar um endpoint da VPC como pré-requisito. Isso ajuda a GuardDuty receber os eventos de tempo de execução. Depois disso, você pode instalar o agente de segurança para que ele comece GuardDuty a receber os eventos de tempo de execução

dos recursos do Amazon EKS. Ao GuardDuty lançar uma nova versão do agente para esse recurso, você pode atualizar a versão do agente em sua conta.

Tópicos

- Pré-requisito — Como criar um endpoint da VPC da Amazon
- Instalação manual do agente de GuardDuty segurança nos recursos do Amazon EKS
- Atualização manual do agente de segurança para recursos do Amazon EKS

Pré-requisito — Como criar um endpoint da VPC da Amazon

Antes de instalar o agente de GuardDuty segurança, você deve criar um endpoint da Amazon Virtual Private Cloud (Amazon VPC). Isso ajudará a GuardDuty receber os eventos de tempo de execução dos seus recursos do Amazon EKS.

> **Note**
>
> Não há custo adicional para usar o endpoint da VPC.

Escolha um método de acesso preferido para criar um endpoint da Amazon VPC.

Console

Para criar um endpoint da VPC

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No menu à de navegação, em Nuvem privada virtual, escolha Endpoints.
3. Escolha Criar endpoint.
4. Na página Criar endpoint, para a Categoria de serviço, escolha Outros serviços de endpoint.
5. Em Nome do serviço, digite **`com.amazonaws.`*`us-east-1`*`.guardduty-data`**.

   Certifique-se de *`us-east-1`* substituir pela região correta. Essa deve ser a mesma região do cluster EKS que pertence ao seu Conta da AWS ID.
6. Selecione Verificar serviço.
7. Depois que o nome do serviço for verificado com sucesso, escolha a VPC em que reside o cluster. Adicione a política a seguir para restringir o uso do endpoint da VPC somente à conta especificada. Com a `Condition` da organização fornecida abaixo desta política, você

pode atualizar a política a seguir para restringir o acesso ao seu endpoint. Para fornecer suporte de endpoint da VPC para IDs de conta específicos em sua organização, consulte Organization condition to restrict access to your endpoint.

JSON

```
{
 "Version":"2012-10-17",
 "Statement": [
  {
   "Action": "*",
   "Resource": "*",
   "Effect": "Allow",
   "Principal": "*"
  },
  {
   "Condition": {
    "StringNotEquals": {
     "aws:PrincipalAccount": "111122223333"
    }
   },
   "Action": "*",
   "Resource": "*",
   "Effect": "Deny",
   "Principal": "*"
  }
 ]
}
```

O ID de conta `aws:PrincipalAccount` deve corresponder à conta que contém a VPC e o endpoint da VPC. A lista a seguir mostra como compartilhar o endpoint da VPC com outros IDs de Conta da AWS :

Condição da organização para restringir o acesso ao endpoint

- Para especificar várias contas para acessar o endpoint da VPC, substitua `"aws:PrincipalAccount": "111122223333"` pelo seguinte:

```
"aws:PrincipalAccount": [
          "666666666666",
```

```
            "555555555555"
        ]
```

- Para permitir que todos os membros de uma organização acessem o endpoint da VPC, substitua `"aws:PrincipalAccount": "111122223333"` pelo seguinte:

```
"aws:PrincipalOrgID": "o-abcdef0123"
```

- Para restringir o acesso para um recurso a um ID de organização, adicione seu `ResourceOrgID` à política.

  Para obter mais informações, consulte ResourceOrgID.

```
"aws:ResourceOrgID": "o-abcdef0123"
```

8. Em Configurações adicionais, selecione Habilitar nome DNS.
9. Em Sub-redes, escolha as sub-redes em que reside seu cluster.
10. Em Grupos de segurança, escolha um grupo de segurança que tenha a porta de entrada 443 habilitada em sua VPC (ou em seu cluster do EKS). Crie um grupo de segurança se ainda não tiver um com uma porta de entrada 443 habilitada.

    Se houver um problema ao restringir as permissões de entrada para sua VPC (ou instância), é possível usar a porta de entrada 443 de qualquer endereço IP (`0.0.0.0/0`). No entanto, GuardDuty recomenda o uso de endereços IP que correspondam ao bloco CIDR da sua VPC. Para obter mais informações, consulte Blocos VPC CIDR no Guia do usuário da Amazon VPC.

API/CLI

Para criar um endpoint da VPC

- Invocar. CreateVpcEndpoint
- Use os valores a seguir para os parâmetros.
  - Em Nome do serviço, digite **`com.amazonaws.`*`us-east-1`*`.guardduty-data`**.

    Certifique-se de *`us-east-1`* substituir pela região correta. Essa deve ser a mesma região do cluster EKS que pertence ao seu Conta da AWS ID.
  - Para DNSOptions, habilite a opção de DNS privado definindo-a como `true`.

- Para isso AWS Command Line Interface, consulte create-vpc-endpoint.

Depois de seguir as etapas, verifique em Validando a configuração do endpoint da VPC se o endpoint da VPC foi configurado corretamente.

Instalação manual do agente de GuardDuty segurança nos recursos do Amazon EKS

Esta seção descreve como você pode implantar o agente GuardDuty de segurança pela primeira vez em clusters EKS específicos. Antes de prosseguir com esta seção, verifique se você já configurou os pré-requisitos e habilitou o Monitoramento de runtime para suas contas. O agente GuardDuty de segurança (complemento EKS) não funcionará se você não ativar o Runtime Monitoring.

Escolha seu método de acesso preferido para implantar o agente de GuardDuty segurança pela primeira vez.

Console

1. Abra o console do Amazon EKS em https://console.aws.amazon.com/eks/home#/clusters.
2. Escolha o Nome do cluster.
3. Escolha a guia Add-ons.
4. Escolha Obter mais complementos.
5. Na página Selecionar complementos, escolha Amazon GuardDuty EKS Runtime Monitoring.
6. GuardDuty recomenda escolher a versão mais recente e padrão do agente.
7. Use as configurações padrão na página Definir configurações do complemento selecionado. Se o status do seu complemento EKS for Requer ativação, escolha Ativar GuardDuty. Essa ação abrirá o GuardDuty console para configurar o Runtime Monitoring para suas contas.
8. Depois de configurar o Monitoramento de runtime para suas contas, volte para o console do Amazon EKS. O Status do seu complemento do EKS deveria ter mudado para Pronto para instalar.
9. (Opcional) Fornecendo o esquema de configuração do complemento do EKS

   Para a versão complementar, se você escolher a versão 1.5.0 ou superior, o Runtime Monitoring oferece suporte à configuração de parâmetros específicos do agente. GuardDuty Para obter informações sobre intervalos de parâmetros, consulte Configurar parâmetros do complemento do EKS.

a. Expanda as Configurações opcionais para visualizar os parâmetros configuráveis e seus valores e formato esperados.

b. Defina os parâmetros. Os valores devem estar dentro do intervalo fornecido emConfigurar parâmetros do complemento do EKS.

c. Escolha Salvar alterações para criar o complemento com base na configuração avançada.

d. Para o Método de resolução de conflitos, a opção escolhida será usada para resolver um conflito quando você atualizar o valor de um parâmetro para um valor não padrão. Para obter mais informações sobre as opções listadas, consulte resolveConflicts na Referência da API do Amazon EKS.

10. Escolha Próximo.
11. Na página Revisar e criar, verifique as rotas e escolha Criar rotas.
12. Navegue de volta aos detalhes do cluster e selecione a guia Recursos.
13. Você pode ver os novos pods com o prefixo aws-guardduty-agent.

API/CLI

Você pode configurar o agente complementar do Amazon EKS (`aws-guardduty-agent`) usando uma das seguintes opções:

- Corra CreateAddonpara sua conta.
-

> **Note**
>
> Para o complemento`version`, se você escolher a versão 1.5.0 ou superior, o Runtime Monitoring oferece suporte à configuração de parâmetros específicos do agente. GuardDuty Para obter mais informações, consulte Configurar parâmetros do complemento do EKS.

Use os seguintes valores para os parâmetros de solicitação:

- Em `addonName`, digite `aws-guardduty-agent`.

Você pode usar o AWS CLI exemplo a seguir ao usar valores configuráveis compatíveis com versões complementares `v1.5.0` ou superiores. Certifique-se de substituir os valores do

espaço reservado destacados em vermelho e os `Example.json` associados aos valores configurados.

```
aws eks create-addon --region us-east-1 --cluster-name myClusterName --addon-
name aws-guardduty-agent --addon-version v1.17.1-eksbuild.2 --configuration-
values 'file://example.json'
```

Example.json

```
{
 "priorityClassName": "aws-guardduty-agent.priorityclass-high",
 "dnsPolicy": "Default",
 "resources": {
  "requests": {
   "cpu": "237m",
   "memory": "512Mi"
  },
  "limits": {
   "cpu": "2000m",
   "memory": "2048Mi"
  }
 }
}
```

- Para obter informações sobre a `addonVersion` compatível, consulte Versões do Kubernetes suportadas pelo agente de segurança GuardDuty.

- Como alternativa, você pode usar AWS CLI. Para obter mais informações, consulte create-addon.

Nomes DNS privados para endpoint da VPC

Por padrão, o agente de segurança resolve e se conecta ao nome DNS privado do endpoint da VPC. Para um endpoint não FIPS, seu DNS privado aparecerá no seguinte formato:

Non-FIPS ponto final — `guardduty-data.us-east-1.amazonaws.com`

O Região da AWS,*us-east-1*, mudará com base na sua região.

Atualização manual do agente de segurança para recursos do Amazon EKS

Ao gerenciar o agente GuardDuty de segurança manualmente, você é responsável por atualizá-lo para sua conta. Para receber notificações sobre novas versões do agente, inscreva-se em um RSS feed para GuardDuty versões de lançamento do agente de segurança.

Atualize o agente de segurança para a versão mais recente para se beneficiar do suporte e das melhorias adicionais. Se sua versão atual do agente estiver chegando ao fim do suporte padrão, para continuar usando o Monitoramento de Runtime (ou Monitoramento de Runtime do EKS), atualize para a seguinte versão disponível do agente ou para a mais recente.

Pré-requisito

Antes de atualizar a versão do agente de segurança, verifique se a versão do agente que planeja usar agora é compatível com sua versão do Kubernetes. Para obter mais informações, consulte Versões do Kubernetes suportadas pelo agente de segurança GuardDuty.

Console

1. Abra o console do Amazon EKS em https://console.aws.amazon.com/eks/home#/clusters.
2. Escolha o Nome do cluster.
3. Em Informações do cluster, escolha a Add-onsguia.
4. Add-onsNa guia, selecione Monitoramento de tempo de execução do GuardDuty EKS.
5. Selecione Editar para atualizar os detalhes do agente.
6. Na página Configurar o monitoramento de tempo de execução do GuardDuty EKS, atualize os detalhes.
7. (Opcional) Atualização das configurações opcionais

   Se sua versão do complemento do EKS for 1.5.0 ou superior, você também pode atualizar o esquema de configurações do complemento.

   a. Expanda Configurações opcionais para ver o esquema de configuração.
   b. Atualize os valores dos parâmetros com base no intervalo fornecido em Configurar parâmetros do complemento do EKS.
   c. Escolha Salvar alterações para iniciar a atualização.
   d. Para o Método de resolução de conflitos, a opção escolhida será usada para resolver um conflito quando você atualizar o valor de um parâmetro para um valor não padrão.

Para obter mais informações sobre as opções listadas, consulte resolveConflicts na Referência da API do Amazon EKS.

API/CLI

Para atualizar o agente GuardDuty de segurança para seus clusters do Amazon EKS, consulte Atualização de um complemento.

> **Note**
>
> Para o complementoversion, se você escolher a versão 1.5.0 ou superior, o Runtime Monitoring oferece suporte à configuração de parâmetros específicos do agente. GuardDuty Para obter informações sobre intervalos de parâmetros, consulte Configurar parâmetros do complemento do EKS.

Você pode usar o AWS CLI exemplo a seguir ao usar valores configuráveis compatíveis com as versões complementares 1.5.0 e superiores. Certifique-se de substituir os valores do espaço reservado destacados em vermelho e os `Example.json` associados aos valores configurados.

```
aws eks update-addon --region us-east-1 --cluster-name myClusterName --addon-
name aws-guardduty-agent --addon-version v1.17.1-eksbuild.2 --configuration-
values 'file://example.json'
```

Example.json

```
{
 "priorityClassName": "aws-guardduty-agent.priorityclass-high",
 "dnsPolicy": "Default",
 "resources": {
  "requests": {
   "cpu": "237m",
   "memory": "512Mi"
  },
  "limits": {
   "cpu": "2000m",
   "memory": "2048Mi"
  }
 }
}
```

Se a versão do complemento Amazon EKS for 1.5.0 ou superior e você tiver configurado o esquema de complemento, poderá verificar se os valores aparecem corretamente ou não para o seu cluster. Para obter mais informações, consulte Verificação das atualizações do esquema de configuração.

Configurar parâmetros do agente de GuardDuty segurança (complemento) para o Amazon EKS

Você pode configurar parâmetros específicos do seu agente de GuardDuty segurança para o Amazon EKS. Esse suporte está disponível para a versão 1.5.0 e superior do GuardDuty Security Agent. Para obter informações sobre as versões mais recentes do complemento, consulte GuardDuty versões do agente de segurança para recursos do Amazon EKS.

Por que devo atualizar o esquema de configuração do agente de segurança

> O esquema de configuração do agente GuardDuty de segurança é o mesmo em todos os contêineres em seus clusters do Amazon EKS. Quando os valores padrão não estiverem alinhados com os workloads e o tamanho da instância associados, considere definir as configurações de CPU, de memória, `PriorityClass` e configurações de `dnsPolicy`. Independentemente de como você gerencia o GuardDuty agente para seus clusters do Amazon EKS, você pode configurar ou atualizar a configuração existente desses parâmetros.

Comportamento de configuração do agente automatizado com parâmetros configurados

Quando GuardDuty gerencia o agente de segurança (complemento EKS) em seu nome, ele atualiza o complemento, conforme necessário. GuardDuty definirá o valor dos parâmetros configuráveis como um valor padrão. No entanto, ainda é possível atualizar os parâmetros para o valor desejado. Se isso levar a um conflito, a opção padrão para resolveConflicts é `None`.

Parâmetros e valores configuráveis

Para obter informações sobre as etapas de configuração dos parâmetros do complemento, consulte:

- Instalação manual do agente de GuardDuty segurança nos recursos do Amazon EKS ou
- Atualização manual do agente de segurança para recursos do Amazon EKS

As tabelas a seguir fornecem os intervalos e valores que se pode usar para implantar o complemento Amazon EKS manualmente ou atualizar as configurações existentes do complemento.

Configurações da CPU

Parâmetros	Valor padrão	Intervalo configurável
Solicitações	200 m	Entre 200m e 10000m, ambos inclusive
Limites	1000 m	Entre 200m e 10000m, ambos inclusive
`disableCpuLimits`	`false`	`true` ou `false`

O `disableCpuLimits` parâmetro está disponível para a versão 1.12.1-eksbuild.3 e posterior do agente de GuardDuty segurança. Em versões anteriores, o complemento não suporta esse parâmetro, e as APIs complementares do Amazon EKS (`CreateAddon`,`UpdateAddon`) retornam um erro de validação se você o especificar.

Quando você define como`true`, `disableCpuLimits` o pod do agente de segurança não impõe um limite de CPU. Outras configurações de recursos não são afetadas.

Para desativar os limites da CPU, use a seguinte configuração:

```
{"resources":{"disableCpuLimits":true}}
```

Memory Settings

Parâmetros	Valor padrão	Intervalo configurável
Solicitações	256 milhões	Entre 256 Milhões e 20000 Milhões, ambos inclusive
Limites	1024 milhões	

Configurações do **`PriorityClass`**

Quando GuardDuty cria um complemento do Amazon EKS para você, o atribuído `PriorityClass` é`aws-guardduty-agent.priorityclass`. Isso significa que nenhuma

ação será tomada com base na prioridade do pod do agente. É possível configurar esse parâmetro do complemento escolhendo uma das opções `PriorityClass` a seguir:

`PriorityClass` configurável	Valor do **`preemptionPolicy`**	Descrição **`preemptionPolicy`**	Valor pod
`aws-guardduty-agent.priorityclass`	`Never`	Nenhuma ação	1000000
`aws-guardduty-agent.priorityclass-high`	`PreemptLowerPriority`	A atribuição desse valor impedirá a execução de um pod com o valor de prioridade e menor que o valor do pod do agente.	100000000
`system-cluster-critical` [1]	`PreemptLowerPriority`		2000000000
`system-node-critical` [1]	`PreemptLowerPriority`		2000001000

[1] Kubernetes fornece essas duas opções `PriorityClass` – `system-cluster-critical` e `system-node-critical`. Para obter mais informações, consulte a PriorityClassdocumentação do Kubernetes.

Configurações do **`dnsPolicy`**

Escolha uma das seguintes opções de política DNS que o Kubernetes suporta. Quando nenhuma configuração é especificada, `ClusterFirst` é usado como o valor padrão.

- `ClusterFirst`
- `ClusterFirstWithHostNet`
- `Default`

Para obter informações sobre essas políticas, consulte Política de DNS de Pod na Documentação do Kubernetes.

Verificação das atualizações do esquema de configuração

Depois de configurar os parâmetros, execute as etapas a seguir para verificar se o esquema de configuração foi atualizado:

1. Abra o console do Amazon EKS em https://console.aws.amazon.com/eks/home#/clusters.
2. No painel de navegação, escolha Clusters.
3. Na página Clusters, selecione o Nome do cluster para o qual você deseja verificar as atualizações.
4. Escolha a guia Recursos.
5. No painel Tipos de recursos, em Cargas de trabalho, escolha. DaemonSets
6. Selecione aws-guardduty-agent.
7. Na página aws-guardduty-agent, escolha Visualização bruta para visualizar a resposta JSON não formatada. Verifique se os parâmetros configuráveis exibem o valor informado.

Depois de verificar, mude para o GuardDuty console. Selecione o correspondente Região da AWS e visualize o status da cobertura dos seus clusters do Amazon EKS. Para obter mais informações, consulte Cobertura de runtime e solução de problemas para clusters do Amazon EKS.

Validando a configuração do endpoint da VPC

Depois de instalar o agente de segurança manualmente ou por meio de configuração GuardDuty automatizada, você pode usar este documento para validar a configuração do VPC endpoint. Você também pode usar essas etapas após solucionar qualquer problema de cobertura de runtime para um tipo de recurso. Você pode garantir que as etapas funcionaram conforme o esperado e que o status da cobertura potencialmente apareça como Íntegro.

Use as etapas a seguir para validar se a configuração do endpoint da VPC para seu tipo de recurso está configurada corretamente na conta do proprietário da VPC:

1. Faça login no Console de gerenciamento da AWS e abra o console da Amazon VPC em. https://console.aws.amazon.com/vpc/
2. No painel de navegação, em Nuvem privada virtual, escolha Suas VPCs.
3. Na página Suas VPCs, escolha o CIDR IPv4 associado ao seu ID de VPC.
4. No menu à de navegação, em Nuvem privada virtual, escolha Endpoints.

5. Na tabela Endpoints, selecione a linha que tem o nome do serviço semelhante a com.amazonaws. ***us-east-1***.guardduty-data. A Região (`us-east-1`) pode ser diferente para seu endpoint.
6. Um painel com detalhes do endpoint será exibido. Na guia Grupos de segurança, selecione o link ID de grupo associado para obter mais detalhes.
7. Na tabela Grupos de Segurança, selecione a linha com o ID do grupo de Segurança associado para ver os detalhes.
8. Na guia Regras de entrada, verifique se existe uma política de entrada com o Intervalo de porta como 443 e Origem como o valor copiado do CIDR IPv4. As regras de entrada controlam o tráfego de entrada que pode chegar à instância. A imagem a seguir mostra as regras de entrada para um grupo de segurança associado à VPC usada pelo GuardDuty agente de segurança.

   Se você ainda não tem um grupo de segurança que tenha uma porta de entrada 443 habilitada, crie um grupo de segurança no Guia do usuário do Amazon EC2.

   Se houver um problema ao restringir as permissões de entrada para sua VPC (ou cluster), permita o tráfego de entrada na porta 443 a partir de qualquer endereço IP (0.0.0). 0/0).

A lista a seguir inclui itens que devem ser conhecidos após a instalação ou atualização do agente de segurança.

Avalie a cobertura de runtime

A próxima etapa após instalar ou atualizar seu agente de segurança é avaliar a cobertura de runtime de seus recursos. Se o status da cobertura de runtime for Não íntegro, você deverá solucionar o problema. Para obter mais informações, consulte Problemas de cobertura de runtime e solução de problemas.

Se o status da cobertura de runtime exibir Íntegro, isso indica que o Monitoramento de runtime consegue coletar e receber os eventos de runtime. Para obter uma lista desses eventos, consulte Tipos de eventos de runtime coletados.

Nome DNS privado para endpoint

Depois de instalar o agente GuardDuty de segurança para seus recursos, por padrão, ele resolverá e se conectará ao nome DNS privado do VPC endpoint. Para um endpoint não FIPS, o DNS privado aparecerá no seguinte formato:

`guardduty-data.`***`us-east-1`***`.amazonaws.com`

O Região da AWS,`us-east-1`, mudará com base na sua região.

Um host pode ser instalado com dois agentes de segurança

Ao trabalhar com o agente de GuardDuty segurança para uma instância do Amazon EC2, você pode instalar e usar o agente no host subjacente dentro de um cluster do Amazon EKS. Caso já tenha implantado um agente de segurança nesse cluster EKS, o mesmo host poderia ter dois agentes de segurança em execução simultaneamente. Para obter informações sobre como GuardDuty funciona nesse cenário, consulteAtendentes de segurança no mesmo host.

Analisando estatísticas de cobertura de runtime e solucionando problemas

Depois de habilitar o Runtime Monitoring e o agente de GuardDuty segurança ser implantado em seu recurso, GuardDuty fornece estatísticas de cobertura para o tipo de recurso correspondente e status de cobertura individual para os recursos que pertencem à sua conta. O status da cobertura é determinado pela garantia de que você habilitou o Runtime Monitoring, que seu endpoint Amazon VPC foi criado e que o agente de GuardDuty segurança do recurso correspondente foi implantado. Um status de cobertura saudável indica que, quando há um evento de tempo de execução relacionado ao seu recurso, GuardDuty é capaz de receber esse evento de tempo de execução por meio do endpoint da Amazon VPC e monitorar o comportamento. Se houve um problema no momento da configuração do Runtime Monitoring, da criação de um endpoint da Amazon VPC ou da implantação do agente de segurança, GuardDuty o status da cobertura aparecerá como Não íntegro. Quando o status da cobertura não estiver íntegro, não GuardDuty poderá receber ou monitorar o comportamento de tempo de execução do recurso correspondente nem gerar nenhuma descoberta do Runtime Monitoring.

Os tópicos a seguir ajudarão você a analisar as estatísticas de cobertura, configurar EventBridge notificações e solucionar os problemas de cobertura de um tipo específico de recurso.

Conteúdo

- Cobertura de runtime e solução de problemas para instância do Amazon EC2
- Cobertura de tempo de execução e solução de problemas para ECS-EC2 Bottlerocket
- Cobertura de runtime e solução de problemas para clusters do Amazon ECS
- Cobertura de runtime e solução de problemas para clusters do Amazon EKS

Cobertura de runtime e solução de problemas para instância do Amazon EC2

Para um recurso Amazon EC2, a cobertura de runtime é avaliada no nível da instância. Suas instâncias do Amazon EC2 podem executar vários tipos de aplicativos e workloads em seu ambiente AWS . Esse atributo também suporta instâncias do Amazon EC2 gerenciadas pelo Amazon EC2 e, se você tiver clusters do Amazon ECS em execução em uma instância do Amazon EC2, os problemas de cobertura no nível da instância aparecerão na cobertura de runtime do Amazon EC2.

Tópicos

- Análise de estatísticas de cobertura
- Alteração do status da cobertura com EventBridge notificações
- Solucionando problemas de cobertura de runtime do Amazon EC2

Análise de estatísticas de cobertura

As estatísticas de cobertura das instâncias do Amazon EC2 associadas às suas próprias contas ou contas-membro são a porcentagem das instâncias do EC2 íntegras em relação a todas as instâncias do EC2 nas Região da AWS selecionadas. A seguinte equação representa isso como:

(instances/All Instâncias íntegras) *100

Se você também implantou o agente de GuardDuty segurança para seus clusters do Amazon ECS, qualquer problema de cobertura no nível da instância associado aos clusters do Amazon ECS executados em uma instância do Amazon EC2 aparecerá como um problema de cobertura de tempo de execução da instância do Amazon EC2.

Selecione um dos métodos de acesso para revisar as estatísticas de cobertura de suas contas.

Console

- Faça login no Console de gerenciamento da AWS e abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.
- No painel de navegação, escolha Monitoramento de runtime.
- Escolha a guia Cobertura de runtime.

- Na guia Cobertura de runtime da instância EC2, é possível visualizar as estatísticas de cobertura agregadas pelo status de cobertura de cada instância do Amazon EC2 que está disponível na tabela Lista de instâncias.
  - Você pode filtrar a tabela Lista de instância pelas seguintes colunas:
    - ID da conta
    - Tipo de gerenciamento de agentes
    - Versão do agente
    - Status da cobertura
    - ID da instância
    - ARN do cluster
- Se alguma das suas instâncias do EC2 tiver o Status de cobertura como Não íntegro, a coluna Problema incluirá informações adicionais sobre o motivo para o status Não íntegro.

API/CLI

- Execute a ListCoverageAPI com seu próprio ID de detector válido, região atual e endpoint de serviço. É possível filtrar e classificar a lista de instâncias utilizando essa API.
  - Você pode alterar o `filter-criteria` de exemplo com uma das seguintes opções para `CriterionKey`:
    - `ACCOUNT_ID`
    - `RESOURCE_TYPE`
    - `COVERAGE_STATUS`
    - `AGENT_VERSION`
    - `MANAGEMENT_TYPE`
    - `INSTANCE_ID`
    - `CLUSTER_ARN`
  - Quando o `filter-criteria` inclui `RESOURCE_TYPE` como EC2, o Monitoramento de runtime não suporta o uso de ISSUE como `AttributeName`. Ao usá-lo, a resposta da API resultará em`InvalidInputException`.

    Você pode alterar o `AttributeName` de exemplo em `sort-criteria` com uma das seguintes opções:
    - `ACCOUNT_ID`

    - COVERAGE_STATUS
    - INSTANCE_ID
    - UPDATED_AT
  - Você pode alterar o *max-results* (até 50).
  - Para encontrar a opção detectorId para sua conta e região atual, consulte a página de configurações no https://console.aws.amazon.com/guardduty/console ou execute a ListDetectorsAPI.

```
aws guardduty --region us-east-1 list-coverage --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --sort-criteria '{"AttributeName":
 "EKS_CLUSTER_NAME", "OrderBy": "DESC"}' --filter-criteria
 '{"FilterCriterion":[{"CriterionKey":"ACCOUNT_ID", "FilterCondition":
{"EqualsValue":"111122223333"}}] }'  --max-results 5
```

- Execute a GetCoverageStatisticsAPI para recuperar estatísticas agregadas de cobertura com base no. statisticsType
  - Você pode alterar o statisticsType de exemplo com uma das seguintes opções:
    - COUNT_BY_COVERAGE_STATUS: representa estatísticas de cobertura para clusters do EKS agregadas por status de cobertura.
    - COUNT_BY_RESOURCE_TYPE— Estatísticas de cobertura agregadas com base no tipo de AWS recurso na lista.
    - Você pode alterar o filter-criteria de exemplo no comando. É possível usar as seguintes opções para CriterionKey:
      - ACCOUNT_ID
      - RESOURCE_TYPE
      - COVERAGE_STATUS
      - AGENT_VERSION
      - MANAGEMENT_TYPE
      - INSTANCE_ID
      - CLUSTER_ARN
  - Para encontrar a opção detectorId para sua conta e região atual, consulte a página de configurações no https://console.aws.amazon.com/guardduty/console ou execute a ListDetectorsAPI.

```
aws guardduty --region us-east-1 get-coverage-statistics --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --statistics-type COUNT_BY_COVERAGE_STATUS
 --filter-criteria '{"FilterCriterion":[{"CriterionKey":"ACCOUNT_ID",
 "FilterCondition":{"EqualsValue":"123456789012"}}] }'
```

Se o status de cobertura da sua instância EC2 é Não íntegro, consulte Solucionando problemas de cobertura de runtime do Amazon EC2.

Alteração do status da cobertura com EventBridge notificações

O status da cobertura da sua instância Amazon ECS pode aparecer como Não íntegro. Para saber quando o status de cobertura é alterado, recomendamos monitorar o status de cobertura periodicamente e solucionar o problema, se o status se tornar Não íntegro. Como alternativa, você pode criar uma EventBridge regra da Amazon para receber uma notificação quando o status da cobertura mudar de Insalubre para Saudável ou não. Por padrão, GuardDuty publica isso no EventBridge barramento da sua conta.

Exemplo de esquema de notificação

Em uma EventBridge regra, você pode usar os exemplos de eventos e padrões de eventos predefinidos para receber a notificação do status da cobertura. Para obter mais informações sobre a criação de uma EventBridge regra, consulte Criar regra no Guia EventBridge do usuário da Amazon.

Além disso, você pode criar um padrão de evento personalizado usando o exemplo de esquema de notificação a seguir. Substitua os valores da sua conta. Para ser notificado quando o status da cobertura da sua instância do Amazon EC2 mudar de `Healthy` para`Unhealthy`, `detail-type` deveria ser. *`GuardDuty Runtime Protection Unhealthy`* Para ser notificado quando o status da cobertura mudar de `Unhealthy` para`Healthy`, substitua o valor de `detail-type` por*`GuardDuty Runtime Protection Healthy`*.

```
{
  "version": "0",
  "id": "event ID",
  "detail-type": "GuardDuty Runtime Protection Unhealthy",
  "source": "aws.guardduty",
  "account": "Conta da AWS ID",
  "time": "event timestamp (string)",
  "region": "Região da AWS",
  "resources": [
```

```
        ],
  "detail": {
    "schemaVersion": "1.0",
    "resourceAccountId": "string",
    "currentStatus": "string",
    "previousStatus": "string",
    "resourceDetails": {
        "resourceType": "EC2",
        "ec2InstanceDetails": {
          "instanceId":"",
          "instanceType":"",
          "clusterArn": "",
          "agentDetails": {
            "version":""
          },
          "managementType":""
        }
    },
    "issue": "string",
    "lastUpdatedAt": "timestamp"
  }
}
```

Solucionando problemas de cobertura de runtime do Amazon EC2

Se o status da cobertura da sua instância do Amazon EC2 for Não íntegra, você poderá ver o motivo na coluna Problema.

Caso sua instância EC2 esteja associada a um cluster EKS e o agente de segurança para EKS tenha sido instalado manualmente ou por meio da configuração automatizada do agente, para solucionar o problema de cobertura, consulte Cobertura de runtime e solução de problemas para clusters do Amazon EKS.

A tabela a seguir lista os tipos de problema e as etapas de solução dos respectivos problemas.

Tipo de problema	Emitir mensagem	Etapas de solução de problemas
Atendente não sendo relatado	Aguardando a notificação do SSM	O recebimento da notificação do SSM pode demorar alguns minutos.

Tipo de problema	Emitir mensagem	Etapas de solução de problemas
		Verifique se a instância Amazon EC2 será administr ada por SSM. Para obter mais informações, consulte as etapas em Método 1 - Usando o AWS Systems Manager emInstalando o agente de segurança manualmente.
	(Intencionalmente vazio)	Se você estiver gerencian do o agente de GuardDuty segurança manualmente, certifique-se de seguir as etapas abaixoGerencian do o agente de segurança manualmente para o recurso do Amazon EC2.
		Caso tenha ativado a configuração automatizada do agente: • A sua instância do EC2 é gerenciada pelo SSM. • Visualize o status do agente de segurança periodicamente. Para obter mais informações, consulte Validando o status GuardDuty de instalação do agente de segurança.

Tipo de problema	Emitir mensagem	Etapas de solução de problemas
		Valide se o endpoint da VPC da sua instância do Amazon EC2 está configura do corretamente. Para obter mais informações, consulte Validando a configuração do endpoint da VPC.
		Se sua organização tiver uma política de controle de serviços (SCP), valide se o limite de permissões não está restringindo a permissão `guardduty:SendSecurityTelemetry` . Para obter mais informações, consulte Validando a política de controle de serviço da sua organização em um ambiente de várias contas.

Tipo de problema	Emitir mensagem	Etapas de solução de problemas
	Atendente desconectado	• Visualize o status do agente de segurança. Para obter mais informações, consulte Validando o status GuardDuty de instalação do agente de segurança. • Visualize os logs do agente de segurança para identific ar a possível causa raiz. Os logs fornecem os detalhes dos erros que podem ser usados para solucionar o problema autonomamente. Esses arquivos de log estão disponíveis em `/var/log/amzn-guardduty-agent/` . Faça `sudo journalctl -u amazon-guardduty-agent` .
Agente não provisionado	As instâncias com tags de exclusão são excluídas do Monitoramento de Runtime.	GuardDuty não recebe eventos de tempo de execução de instâncias do Amazon EC2 que são iniciadas com a tag de exclusão:. `GuardDuty Managed false` Para receber eventos de runtime dessa instância do Amazon EC2, remova a tag de exclusão.

Tipo de problema	Emitir mensagem	Etapas de solução de problemas
	A versão do kernel é inferior à versão compatível.	Para obter informações sobre as versões do kernel compatíveis em todas as distribuições do sistema operacional, consulte Validação dos requisitos de arquitetura para as instâncias do Amazon EC2.
	A versão do kernel é superior à versão compatível.	Para obter informações sobre as versões do kernel compatíveis em todas as distribuições do sistema operacional, consulte Validação dos requisitos de arquitetura para as instâncias do Amazon EC2.

Tipo de problema	Emitir mensagem	Etapas de solução de problemas
	Não é possível recuperar o documento de identidade da instância.	Siga estas etapas: 1. Confirme se seu recurso é uma instância do Amazon EC2 e não uma instância híbrida que não seja do EC2. 2. Confirme se o serviço de metadados de instância (IMDS) está habilitado. Para isso, consulte Configurar opções de serviço de metadados de instância no Guia do usuário do Amazon EC2. 3. Verifique se o documento de identidade da instância existe. Para isso, consulte Recuperar o documento de identidade da instância no Guia do usuário do Amazon EC2. 4. Se o documento de identidade da instância ainda não existir, reinicie a instância. O documento de identidade da instância é gerado quando a instância é interrompida e iniciada, reiniciada ou lançada.

Tipo de problema	Emitir mensagem	Etapas de solução de problemas
Falha na criação da associação do SSM	GuardDuty A associação SSM já existe em sua conta	1. Excluir a associação atual manualmente. Para obter mais informações, consulte Excluindo associações no Guia do usuário AWS Systems Manager 2. Depois de excluir a associação, desative e reative a configuração GuardDuty automática do agente para o Amazon EC2.
	Sua conta tem muitas associações do SSM	Escolha uma das seguintes duas opções: • Excluir todas as associações do SSM não utilizadas. Para obter mais informações, consulte Excluindo associações no Guia do usuário AWS Systems Manager • Verifique se sua conta se qualifica para um aumento de cota. Para obter informações, consulte as cotas do Systems Manager no Referência geral da AWS.

Tipo de problema	Emitir mensagem	Etapas de solução de problemas
Falha na atualização da associação SSM	GuardDuty A associação SSM não existe em sua conta	GuardDuty A associação SSM não está presente em sua conta. Desabilite e, em seguida, reabilite o Monitoramento de runtime.
Falha na exclusão da associação SSM	GuardDuty A associação SSM não existe em sua conta	A associação SSM não está presente em sua conta. Caso a associação do SSM tenha sido excluída intencionalmente, nenhuma ação será necessária.

Tipo de problema	Emitir mensagem	Etapas de solução de problemas
Falha na execução da associação de instância do SSM	Os requisitos arquitetônicos ou outros pré-requisitos não foram atendidos.	Para obter informações sobre distribuições verificadas do sistema operacional, consulte Pré-requisitos para suporte de instância do Amazon EC2. Caso esse problema persista, as etapas a seguir ajudarão a identificar e possivelmente resolver o problema: 1. Abra o AWS Systems Manager console em https://console.aws.amazon.com/systems-manager/. 2. No painel de navegação, em Gerenciamento de nó, selecione State Manager. 3. Filtrar por Nome do documento e digitar AmazonGuardDuty-ConfigureRuntimeMonitoringSsmPlugin. 4. Selecione o ID da associação correspondente e visualize seu Histórico de execução. 5. Usando o histórico de execução, visualize as falhas, identifique a possível causa raiz e tente resolvê-la.

Tipo de problema	Emitir mensagem	Etapas de solução de problemas
Falha na criação de endpoint da VPC	A criação de VPC endpoint não é compatível com VPC compartilhada *vpcId*	O Monitoramento de runtime suporta o uso de uma VPC compartilhada em uma organização. Para obter mais informações, consulte Como usar uma VPC compartilhada com Monitoramento de Runtime.
	Somente ao usar VPC compartilhada com configuração de agente automatizado O ID da conta do *111122223333* proprietário da VPC compartilhada *vpcId* não tem o Runtime Monitoring, a configuração automatizada do agente ou ambos ativados	A conta compartilhada do proprietário da VPC deve habilitar o Monitoramento de runtime e a configuração de agente automatizado para pelo menos um tipo de recurso (Amazon EKS ou Amazon ECS (AWS Fargate)). Para obter mais informações, consulte Pré-requisitos específicos para o monitoramento de tempo de execução GuardDuty.

Tipo de problema	Emitir mensagem	Etapas de solução de problemas
	A ativação do DNS privado requer ambos `enableDnsSupport` e os atributos da `enableDnsHostnames` VPC definidos `true` como *`vpcId`* for (Serviço: Ec2, Code:400 Status, ID da solicitação:). *`a1b2c3d4-5678-90ab-cdef-EXAMPLE11111`*	Verifique se os seguintes atributos da VPC estão definidos como `true`: `enableDnsSupport` e `enableDnsHostnames`. Para obter mais informações, consulte Atributos de DNS na sua VPC. Se você estiver usando o Amazon VPC Console em https://console.aws.amazon.com/vpc/para criar o Amazon VPC, selecione Habilitar nomes de host DNS e Ativar resolução de DNS. Para obter mais informações, consulte Opções de configuração da VPC. Depois de atualizar os atributos da VPC, você deve acelerar uma nova tentativa da criação do endpoint da VPC fazendo uma das seguintes alterações: • Você pode adicionar ou modificar a tag `GuardDuty Managed` para sua instância do Amazon EC2 (recomendado). Por exemplo, você pode adicionar `GuardDuty`

Tipo de problema	Emitir mensagem	Etapas de solução de problemas
		`Managed :true` para incluir a instância para o Monitoramento de Runtime. • Você pode alterar o estado da instância do Amazon EC2 (parar ou reiniciar).

Tipo de problema	Emitir mensagem	Etapas de solução de problemas
Falha na exclusão de endpoint da VPC compartilhada	A exclusão compartilhada do VPC endpoint não é permitida para ID da conta, *vpcId* VPC *111122223333* compartilhada e ID da conta do proprietário. *555555555555*	Etapas possíveis: • A desativação do status de Monitoramento de runtime da conta de participante da VPC compartilhada não afeta a política de endpoint da VPC compartilhada e o grupo de segurança que existe na conta do proprietário. Para excluir o grupo de segurança e endpoint da VPC compartilhada, desative o Monitoramento de runtime ou o status de configuração de agente automatizado na conta do proprietário da VPC compartilhada. • A conta do participante da VPC compartilhada não pode excluir o grupo de segurança e o endpoint da VPC compartilhada hospedados na conta compartilhada do proprietário da VPC.

Tipo de problema	Emitir mensagem	Etapas de solução de problemas
Agente não sendo relatado	(Intencionalmente vazio)	Não há mais suporte para o tipo de problema. Se você continuar enfrentando esse problema e ainda não o fez, habilite o agente GuardDuty automatizado para o Amazon EC2. Se o problema ainda persistir , considere desabilitar o Monitoramento de runtime por alguns minutos e depois habilitá-lo novamente.

Cobertura de tempo de execução e solução de problemas para ECS-EC2 Bottlerocket

Para instâncias Bottlerocket do Amazon EC2 em clusters do Amazon ECS GuardDuty , avalia a cobertura do tempo de execução no nível da instância. O agente GuardDuty de segurança é executado como um contêiner host no Bottlerocket, e não como um pacote RPM ou Debian instalado.

As instâncias Bottlerocket do Amazon EC2 aparecem na guia Cobertura de tempo de execução da instância EC2. Para revisar as estatísticas de cobertura de suas instâncias do Bottlerocket, abra o GuardDuty console, escolha Runtime Monitoring no painel de navegação e, em seguida, escolha a guia Cobertura em tempo de execução. Em Cobertura de tempo de execução da instância EC2, você pode visualizar o status da cobertura de cada instância e filtrar por ID da conta, versão do agente ou status da cobertura. Para obter mais informações, consulte Análise de estatísticas de cobertura.

Solução de problemas de cobertura de tempo de execução do Bottlerocket ECS-EC2

Se o status da cobertura da sua instância Bottlerocket Amazon EC2 for Insalubre, você poderá ver o motivo na coluna Problema.

A tabela a seguir lista os tipos de problema e as etapas de solução dos respectivos problemas.

Tipo de problema	Emitir mensagem	Etapas de solução de problemas
Atendente não sendo relatado	Aguardando a notificação do SSM	O recebimento da notificação de SSM pode levar alguns minutos. Certifique-se de que sua instância do Bottlerocket seja gerenciada por SSM. O agente SSM é executado no contêiner de controle Bottlerocket por padrão. Verifique se o perfil da instância inclui `AmazonSSMManagedInstanceCore` as políticas `AmazonEC2ContainerRegistryReadOnly` gerenciadas.
Atendente não sendo relatado	Não aplicável	Verifique se o contêiner do host do agente está ativado e em execução: 1. Conecte-se à sua instância usando o SSM Session Manager. 2. Entre no contêiner de administração:`enter-admin-container` . 3. Verifique as configurações:`apiclient get settings.host-containers.amazon-guardduty-agent` . Confirme que `enabled` é `true` e `superpowered` é`true`.

Tipo de problema	Emitir mensagem	Etapas de solução de problemas
		4. Verifique se o processo do agente está em execução: `sheltie ps aux | grep guardduty` . 5. Verifique os registros do agente usando uma das seguintes opções: • `sheltie journalctl -u host-containers@amazon-guardduty-agent` • De uma sessão do Sheltie (`sudo sheltie`):`ls /var/log/amzn-guardduty-agent/` .
Atendente não sendo relatado	Não aplicável	Valide se a instância tem conectividade de rede com o endpoint Amazon ECR e o GuardDuty VPC endpoint. Se sua instância for executada em uma sub-rede privada, verifique se você configurou endpoints VPC para Amazon ECR e. GuardDuty

Tipo de problema	Emitir mensagem	Etapas de solução de problemas
Atendente não sendo relatado	Não aplicável	Se sua organização tiver uma política de controle de serviços (SCP), confirme se o limite de permissões permite a `guardduty:SendSecurityTelemetry` permissão.
Falha na criação da associação do SSM	GuardDuty A associação SSM já existe em sua conta.	1. Excluir a associação atual manualmente. Para obter mais informações, consulte Excluindo associações no Guia do usuário AWS Systems Manager 2. Depois de excluir a associação, desative e reative a configuração GuardDuty automática do agente para o Amazon EC2.

Tipo de problema	Emitir mensagem	Etapas de solução de problemas
Falha na criação da associação do SSM	Sua conta tem muitas associações de SSM.	Escolha uma das seguintes duas opções: • Excluir todas as associações do SSM não utilizadas. Para obter mais informações, consulte Excluindo associações no Guia do usuário AWS Systems Manager • Verifique se sua conta se qualifica para um aumento de cota. Para obter informações, consulte as cotas do Systems Manager no Referência geral da AWS.
Falha na atualização da associação SSM	GuardDuty A associação SSM não existe em sua conta.	GuardDuty A associação SSM não está presente em sua conta. Desabilite e, em seguida, reabilite o Monitoramento de runtime.
Falha na exclusão da associação SSM	GuardDuty A associação SSM não existe em sua conta.	A associação SSM não está presente em sua conta. Caso a associação do SSM tenha sido excluída intencionalmente, nenhuma ação será necessária.

Tipo de problema	Emitir mensagem	Etapas de solução de problemas
Falha na execução da associação de instância do SSM	Os requisitos arquitetônicos ou outros pré-requisitos não foram atendidos.	Para obter informações sobre os requisitos verificados, consulte Pré-requisitos para o suporte do Bottlerocket ECS-EC2. Se você ainda tiver esse problema, verifique o histórico de execução do SSM State Manager: 1. Abra o AWS Systems Manager console em https://console.aws.amazon.com/systems-manager/. 2. No painel de navegação, em Gerenciamento de nó, selecione State Manager. 3. Filtrar por Nome do documento e digitar AmazonGuardDuty-ConfigureRuntimeMonitoringSsmPlugin. 4. Selecione o ID da associação correspondente e visualize seu Histórico de execução. 5. Usando o histórico de execução, visualize as falhas, identifique a possível causa raiz e tente resolvê-la.

Tipo de problema	Emitir mensagem	Etapas de solução de problemas
Atendente desconectado	Não aplicável	• Verifique os registros do agente no contêiner administrativo: `enter-admin-container sheltie journalctl -u host-containers@amazon-guardduty-agent` • Verifique se a imagem do contêiner do agente foi obtida com sucesso verificando se o `source` campo nas configurações do contêiner do host aponta para um URI válido do Amazon ECR. • Certifique-se de que o perfil da instância tenha permissões de pull do Amazon ECR. Para obter mais informações, consulte Faça com que as instâncias do EC2 sejam gerenciadas por SSM e configure as permissões da instância.

Tipo de problema	Emitir mensagem	Etapas de solução de problemas
Agente não provisionado	As instâncias com tags de exclusão são excluídas do Monitoramento de Runtime.	GuardDuty não recebe eventos de tempo de execução de instâncias do Amazon EC2 que são iniciadas com a tag de exclusão:. `GuardDuty Managed false` Para receber eventos de tempo de execução dessa instância, remova a tag de exclusão.
Agente não provisionado	A versão do kernel é inferior à versão compatível.	Atualize para a última versão do Bottlerocket ou da ECS-3 AMI ECS-2 otimizada `v1.62.1` ou posterior para configuração automatizada do agente.

Tipo de problema	Emitir mensagem	Etapas de solução de problemas
Falha na extração da imagem ECR	A imagem do contêiner do agente não pôde ser retirada do Amazon ECR.	• Verifique se o perfil da instância inclui a política `AmazonEC2ContainerRegistryReadOnly` gerenciada ou as permissões individuais necessárias do Amazon ECR. • Verifique a conectividade da rede com o endpoint do Amazon ECR em sua região. • Se estiver usando uma sub-rede privada, certifique-se de que os VPC endpoints estejam configurados. Para obter mais informações, consulte Requisitos de conectividade de rede.

Cobertura de runtime e solução de problemas para clusters do Amazon ECS

A cobertura de tempo de execução dos clusters do Amazon ECS inclui as tarefas em execução nas AWS Fargate instâncias de contêineres do Amazon ECS. [1]

Para um cluster do Amazon ECS executado no Fargate, a cobertura do runtime é avaliada no nível da tarefa. A cobertura de runtime dos clusters ECS inclui as tarefas do Fargate que começaram a ser executadas depois que o Monitoramento de runtime e a configuração de agente automatizado foram habilitados para o Fargate (somente ECS). Por padrão, uma tarefa do Fargate é imutável. GuardDuty não será possível instalar o agente de segurança para monitorar contêineres em tarefas já em execução. Para incluir essa tarefa do Fargate, pare e inicie a tarefa novamente. Verifique se o serviço associado é compatível.

Para obter informações sobre o contêiner do Amazon ECS, consulte Criação de capacidade.

Conteúdo

- Análise de estatísticas de cobertura
- Alteração do status da cobertura com EventBridge notificações
- Solução de problemas de cobertura ECS-Fargate de tempo de execução da Amazon

Análise de estatísticas de cobertura

As estatísticas de cobertura dos recursos do Amazon ECS associados às suas próprias contas ou contas-membro são a porcentagem dos clusters do Amazon ECS íntegros em relação a todos os clusters do Amazon ECS nas Região da AWS selecionadas. Isso inclui a cobertura para clusters do Amazon ECS associados às instâncias do Fargate e do Amazon EC2. A seguinte equação representa isso como:

(clusters/All Clusters saudáveis) *100

Considerações

- As estatísticas de cobertura do cluster do ECS incluem o status de cobertura das tarefas do Fargate ou das instâncias de contêiner do ECS associadas a esse cluster do ECS. O status de cobertura das tarefas do Fargate inclui tarefas que estão em execução ou que foram concluídas recentemente.
- Na guia Cobertura de tempo de execução dos clusters ECS, o campo Container instances covered indica o status da cobertura das instâncias de contêiner do Amazon EC2 associadas ao seu cluster do Amazon ECS.

  Se o seu cluster do Amazon ECS executar somente o tipo de execução do Fargate, esse campo exibirá um traço (-) para indicar que a contagem não é aplicável. Um Fargate-only cluster não tem instâncias de contêiner do Amazon EC2 para cobrir.
- Se o seu cluster do Amazon ECS estiver associado a uma instância do Amazon EC2 que não tenha um agente de segurança, o cluster do Amazon ECS também terá um status de cobertura Não íntegro.

  Para identificar e solucionar o problema de cobertura da instância associada do Amazon EC2, consulte Solucionando problemas de cobertura de runtime do Amazon EC2 para instâncias do Amazon EC2.

Selecione um dos métodos de acesso para revisar as estatísticas de cobertura de suas contas.

Console

- Faça login no Console de gerenciamento da AWS e abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.
- No painel de navegação, escolha Monitoramento de runtime.
- Escolha a guia Cobertura de runtime.
- Na guia Cobertura de runtime de clusters ECS, você pode visualizar as estatísticas de cobertura agregadas pelo status de cobertura de cada cluster Amazon ECS disponível na tabela Lista de clusters.
  - Você pode filtrar a tabela Lista de clusters pelas seguintes colunas:
    - ID da conta
    - Nome do cluster
    - Tipo de gerenciamento de agentes
    - Status da cobertura
- Se algum dos seus clusters do Amazon ECS tiver o Status de cobertura como Não íntegro, a coluna Problema incluirá informações adicionais sobre o motivo do status Não íntegro.

  Se seus clusters do Amazon ECS estiverem associados a uma instância do Amazon EC2, navegue até a guia Cobertura de runtime da instância do EC2 e filtre pelo campo Nome do cluster para visualizar o Problema associado.

API/CLI

- Execute a ListCoverageAPI com seu próprio ID de detector válido, região atual e endpoint de serviço. É possível filtrar e classificar a lista de instâncias utilizando essa API.
  - Você pode alterar o `filter-criteria` de exemplo com uma das seguintes opções para `CriterionKey`:
    - `ACCOUNT_ID`
    - `ECS_CLUSTER_NAME`
    - `COVERAGE_STATUS`
    - `MANAGEMENT_TYPE`

- Você pode alterar o `AttributeName` de exemplo em `sort-criteria` com uma das seguintes opções:
  - `ACCOUNT_ID`
  - `COVERAGE_STATUS`
  - `ISSUE`
  - `ECS_CLUSTER_NAME`
  - `UPDATED_AT`

    O campo é atualizado somente quando uma nova tarefa é criada no cluster associado do Amazon ECS ou quando ocorre uma alteração no status da respectiva cobertura.
- Você pode alterar o *`max-results`* (até 50).
- Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no https://console.aws.amazon.com/guardduty/console ou execute a ListDetectorsAPI.

```
aws guardduty --region us-east-1 list-coverage --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --sort-criteria '{"AttributeName":
 "ECS_CLUSTER_NAME", "OrderBy": "DESC"}' --filter-criteria
 '{"FilterCriterion":[{"CriterionKey":"ACCOUNT_ID", "FilterCondition":
{"EqualsValue":"111122223333"}}] }'  --max-results 5
```

- Execute a GetCoverageStatisticsAPI para recuperar estatísticas agregadas de cobertura com base no. `statisticsType`
  - Você pode alterar o `statisticsType` de exemplo com uma das seguintes opções:
    - `COUNT_BY_COVERAGE_STATUS` – representa estatísticas de cobertura para clusters do ECS agregadas por status de cobertura.
    - `COUNT_BY_RESOURCE_TYPE`— Estatísticas de cobertura agregadas com base no tipo de AWS recurso na lista.
    - Você pode alterar o `filter-criteria` de exemplo no comando. É possível usar as seguintes opções para `CriterionKey`:
      - `ACCOUNT_ID`
      - `ECS_CLUSTER_NAME`
      - `COVERAGE_STATUS`
      - `MANAGEMENT_TYPE`

    - `INSTANCE_ID`
- Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no https://console.aws.amazon.com/guardduty/console ou execute a ListDetectorsAPI.

```
aws guardduty --region us-east-1 get-coverage-statistics --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --statistics-type COUNT_BY_COVERAGE_STATUS
 --filter-criteria '{"FilterCriterion":[{"CriterionKey":"ACCOUNT_ID",
 "FilterCondition":{"EqualsValue":"123456789012"}}] }'
```

Para obter mais informações sobre esses problemas de cobertura, consulte Solução de problemas de cobertura ECS-Fargate de tempo de execução da Amazon.

Alteração do status da cobertura com EventBridge notificações

O status da cobertura do seu cluster Amazon ECS pode aparecer como Não íntegro. Para saber quando o status de cobertura é alterado, recomendamos monitorar o status de cobertura periodicamente e solucionar o problema, se o status se tornar Não íntegro. Como alternativa, você pode criar uma EventBridge regra da Amazon para receber uma notificação quando o status da cobertura mudar de Insalubre para Saudável ou não. Por padrão, GuardDuty publica isso no EventBridge barramento da sua conta.

Exemplo de esquema de notificação

Em uma EventBridge regra, você pode usar os exemplos de eventos e padrões de eventos predefinidos para receber a notificação do status da cobertura. Para obter mais informações sobre a criação de uma EventBridge regra, consulte Criar regra no Guia EventBridge do usuário da Amazon.

Além disso, você pode criar um padrão de evento personalizado usando o exemplo de esquema de notificação a seguir. Substitua os valores da sua conta. Para ser notificado quando o status da cobertura do seu cluster Amazon ECS mudar de `Healthy` para`Unhealthy`, `detail-type` deveria ser*`GuardDuty Runtime Protection Unhealthy`*. Para ser notificado quando o status da cobertura mudar de `Unhealthy` para`Healthy`, substitua o valor de `detail-type` por*`GuardDuty Runtime Protection Healthy`*.

```
{
  "version": "0",
  "id": "event ID",
```

```
  "detail-type": "GuardDuty Runtime Protection Unhealthy",
  "source": "aws.guardduty",
  "account": "Conta da AWS ID",
  "time": "event timestamp (string)",
  "region": "Região da AWS",
  "resources": [
       ],
  "detail": {
    "schemaVersion": "1.0",
    "resourceAccountId": "string",
    "currentStatus": "string",
    "previousStatus": "string",
    "resourceDetails": {
        "resourceType": "ECS",
        "ecsClusterDetails": {
          "clusterName":"",
          "fargateDetails":{
            "issues":[],
            "managementType":""
          },
          "containerInstanceDetails":{
            "coveredContainerInstances":int,
            "compatibleContainerInstances":int
          }
        }
    },
    "issue": "string",
    "lastUpdatedAt": "timestamp"
  }
}
```

Solução de problemas de cobertura ECS-Fargate de tempo de execução da Amazon

Se o status da cobertura do seu cluster Amazon ECS for Não íntegro, você poderá ver o motivo na coluna Problema.

A tabela a seguir fornece as etapas recomendadas para a solução de problemas do Fargate (somente Amazon ECS). Para obter informações sobre problemas de cobertura de instância do Amazon EC2, consulte Solucionando problemas de cobertura de runtime do Amazon EC2 para instâncias do Amazon EC2.

Tipo de problema	Informações adicionais	Etapas para solução de problemas
Agente não sendo relatado		Valide se o endpoint da VPC para a tarefa do seu cluster Amazon ECS está configurado corretamente. Para obter mais informações, consulte Validando a configuração do endpoint da VPC.
	Agente não sendo relatado para tarefas em `TaskDefinition - ' TASK_DEFINITION '`	Se sua organização tiver uma política de controle de serviços (SCP), valide se o limite de permissões não está restringindo a permissão `guardduty:SendSecurityTelemetry` . Para obter mais informações, consulte Validando a política de controle de serviço da sua organização em um ambiente de várias contas.
	`VPC_ISSUE ; for task in TaskDefinition - 'TASK_DEFINITION '`	Veja os detalhes do problema da VPC nas informações extra.
Atendente encerrado	ExitCode: `EXIT_CODE` para tarefas em `TaskDefinition - ' TASK_DEFINITION '`	Veja os detalhes do problema nas informações extra.
	Motivo: *REASON* para tarefas em `TaskDefinition - 'TASK_DEFINITION '`	

Tipo de problema	Informações adicionais	Etapas para solução de problemas
	ExitCode: `EXIT_CODE` com o motivo: '*`EXIT_CODE`* ' para tarefas em `TaskDefinition - '` *`TASK_DEFINITION`* '	

Tipo de problema	Informações adicionais	Etapas para solução de problemas
	Atendente encerrado: Motivo: `CannotPullContainerError` : manifesto de imagem pull repetido…	Nesse cenário, GuardDuty é potencialmente incapaz de extrair a imagem do contêiner auxiliar. Sua tarefa continuará em execução, mas não GuardDuty conseguirá detectar possíveis ameaças. Execute as seguintes etapas de solução de problemas, uma de cada vez, para verificar se isso ajuda a resolver o problema de cobertura: • Permissões: verifique se seu perfil de execução de tarefas tem as permissões de ECR necessárias listadas em Requisitos de permissão. • Conectividade de rede: verifique se suas tarefas do Fargate podem alcançar o ECR por meio de acesso público à Internet ou endpoints da VPC configurados adequadamente, conforme descrito em Requisitos de conectividade de rede. • Configuração do grupo de segurança: verifique se seu grupo de segurança permite acesso externo à lista de

Tipo de problema	Informações adicionais	Etapas para solução de problemas
		prefixos gerenciados do S3 na porta 443, conforme explicado em Configuração do security group. • Execute o AWSSupport-TroubleshootECSTaskFailedToStartrunbook na região do seu cluster para identificar problemas específicos. • Examine os logs da tarefa em busca de mensagens de erro. Para obter informaçõ es sobre como fazer isso, consulte Visualizar logs do agente de contêiner do Amazon ECS no Guia do desenvolvedor do Amazon Elastic Container Service. Para erros comuns e soluções de problemas , consulte Solução de problemas do Amazon ECS no Guia do desenvolv edor do Amazon Elastic Container Service. Esses três componentes (permissões, conectividade de rede e configuração do grupo de segurança) são independe ntes, mas são todos necessári

Tipo de problema	Informações adicionais	Etapas para solução de problemas
		os para fazer o download bem-sucedido da imagem do GuardDuty contêiner do Amazon ECR. Se o problema persistir, consulte Meu AWS Step Functions o fluxo de trabalho está falhando inesperad amente.
Falha na criação de endpoint da VPC	A ativação do DNS privado requer ambos `enableDns Support` e os atributos da `enableDnsHostnames` VPC definidos `true` como *`vpcId`* for (Serviço: EC2, Code:400 Status, ID da solicitação:). *`a1b2c3d4-5678-90ab-cdef-EXAMPLE11111`*	Verifique se os seguintes atributos da VPC estão definidos como `true`: `enableDnsSupport` e `enableDnsHostnames` . Para obter mais informações, consulte Atributos de DNS na sua VPC. Se você estiver usando o Amazon VPC Console em https://console.aws.amazon.com/vpc/para criar o Amazon VPC, certifique-se de selecionar Habilitar nomes de host DNS e Ativar resolução de DNS. Para obter mais informações, consulte Opções de configuração da VPC.
Atendente não provisionado	Invocação não suportada por *`SERVICE`* para tarefa(s) em `TaskDefinition -` *`'TASK_DEFINITION '`*	Essa tarefa foi invocada por um *`SERVICE`* que não é compatível.

Tipo de problema	Informações adicionais	Etapas para solução de problemas
	Arquitetura de CPU '*TYPE*' não suportada para tarefas em `TaskDefinition - '`*TASK_DEFINITION* '	Essa tarefa está sendo executada em uma arquitetura de CPU não compatível. Para obter informações sobre as arquiteturas de CPU compatíveis, consulte Validação dos requisitos de arquitetura.
	`TaskExecutionRole` faltando em `TaskDefinition - '` *TASK_DEFINITION* '	A função de execução de tarefa do ECS está ausente. Para obter informações sobre o fornecimento da função de execução de tarefa e permissões necessárias, consulte Pré-requisitos para acesso à imagem do contêiner .

Tipo de problema	Informações adicionais	Etapas para solução de problemas
	Falta configuração de rede '*CONFIGURATION_DETAILS* ' para tarefa(s) em `TaskDefinition -` '*TASK_DEFINITION* '	Problemas de configuração de rede podem aparecer devido à falta de configuração de VPC ou sub-redes ausentes ou vazias. Valide se sua configuração de rede está correta. Para obter mais informações, consulte Pré-requisitos para acesso à imagem do contêiner. Para obter mais informaçõ es, consulte Parâmetros da definição de tarefa do Amazon ECS no Guia do desenvolv edor do Amazon Elastic Container Service.
	As tarefas iniciadas quando os clusters tinham uma tag de exclusão são excluídas do Monitoramento de Runtime. IDs de tarefa afetados: “*TASK_ID*”	Quando você altera a GuardDuty tag predefinida de `GuardDutyManaged -true` para `GuardDutyManaged -false`, não GuardDuty receberá os eventos de tempo de execução desse cluster do Amazon ECS. Atualize a tag para `GuardDutyManaged -true` e reinicie a tarefa.

Tipo de problema	Informações adicionais	Etapas para solução de problemas
	Os serviços implantados quando os clusters tinham uma tag de exclusão são excluídos do Monitoram ento de Runtime. Nomes dos serviços afetados: “*SERVICE_NAME* ”	Quando os serviços são implantados com a tag de exclusão `GuardDuty Managed -false`, não GuardDuty receberão eventos de tempo de execução para esse cluster do Amazon ECS. Atualize a tag para `GuardDutyManaged -true` e depois reimplante o serviço.
	As tarefas iniciadas antes da habilitação da Configuração Automatizada do Agente não são abordadas. IDs de tarefa afetados: “*TASK_ID*”	Quando o cluster contém uma tarefa iniciada antes de ativar a configuração automatizada do agente para o Amazon ECS, não GuardDuty será possível protegê-la. Reinicie a tarefa para que ela seja monitorada por. GuardDuty
	Os serviços implantados antes da habilitação da Configuração Automatizada do Agente não são cobertos. Nomes dos serviços afetados: “*SERVICE_NAME* ”	Quando os serviços são implantados antes de habilitar a configuração automatiz ada de agentes para o Amazon ECS, não GuardDuty receberão eventos de tempo de execução para clusters do ECS.

Tipo de problema	Informações adicionais	Etapas para solução de problemas
	O serviço *SERVICE_NAME* " requer uma nova implantação no fix/troubleshoot. Consulte a documentação. Nomes dos serviços afetados: "*SERVICE_NAME* "	Não há suporte para um serviço iniciado antes de habilitar o Monitoramento de Runtime. Você pode reiniciar o serviço ou atualizá-lo com a opção `forceNewDeployment` seguindo as etapas em Atualizar um serviço do Amazon ECS usando o console no Guia do desenvolvedor do Amazon Elastic Container Service. Como alternativa, você também pode usar as etapas abaixo UpdateServicena Referência de API do Amazon Elastic Container Service.
	As tarefas iniciadas antes da habilitação do Monitoramento de Runtime exigem uma reinicialização. IDs de tarefa afetados: "*TASK_ID_1* "	No Amazon ECS, as tarefas são imutáveis. Para avaliar o comportamento do tempo de execução ou uma AWS Fargate tarefa em execução, verifique se o Runtime Monitoring já está ativado e reinicie a tarefa GuardDuty para adicionar o sidecar do contêiner.

Tipo de problema	Informações adicionais	Etapas para solução de problemas
Outros	Problema não identificado, para tarefas em `TaskDefinition - ' TASK_DEFINITION '`	Use as seguintes questões para identificar a causa raiz do problema: • A tarefa foi iniciada antes de você habilitar o Monitoramento de runtime? No Amazon ECS, as tarefas são imutáveis. Para avaliar o comportamento em tempo de execução de uma tarefa do Fargate em execução, verifique se o Runtime Monitoring já está ativado e reinicie a tarefa para adicionar o GuardDuty sidecar do contêiner. • Essa tarefa faz parte de uma implantação de serviço que começou antes de você ativar o Monitoramento de runtime? Se sim, você pode reiniciar o serviço ou atualizá-lo com `forceNewDeployment` usando as etapas em Atualizando um serviço. Você também pode usar UpdateServiceou AWS CLI.

Tipo de problema	Informações adicionais	Etapas para solução de problemas
		• A tarefa foi iniciada depois de excluir o cluster ECS do Monitoramento de runtime? Quando você altera a GuardDuty tag predefinida de `GuardDutyManaged - true` para `GuardDuty Managed -false`, não GuardDuty receberá os eventos de tempo de execução para o cluster do ECS. • Seu serviço contém uma tarefa que tem um formato antigo de `taskArn`? GuardDuty O Runtime Monitoring não oferece suporte à cobertura de tarefas que têm o formato antigo de`taskArn`. Para obter informaçõ es sobre os nomes dos recursos da Amazon (ARNs) para recursos do Amazon ECS, consulte nomes dos recursos da Amazon (ARNs) e IDs.

Cobertura de runtime e solução de problemas para clusters do Amazon EKS

Depois de ativar o Runtime Monitoring e instalar o agente de GuardDuty segurança (complemento) para EKS manualmente ou por meio da configuração automatizada do agente, você pode começar a avaliar a cobertura dos seus clusters EKS.

Conteúdo

- Análise de estatísticas de cobertura
- Alteração do status da cobertura com EventBridge notificações
- Solucionando problemas de cobertura de runtime do Amazon EKS

Análise de estatísticas de cobertura

As estatísticas de cobertura dos clusters do EKS associados às suas próprias contas ou contas-membro são a porcentagem dos clusters do EKS saudáveis em relação a todos os clusters do EKS nas Região da AWS selecionadas. A seguinte equação representa isso como:

(clusters/All Clusters saudáveis) *100

Selecione um dos métodos de acesso para revisar as estatísticas de cobertura de suas contas.

Console

- Faça login no Console de gerenciamento da AWS e abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.
- No painel de navegação, escolha Monitoramento de runtime.
- Escolha a guia Cobertura de runtime dos clusters do EKS.
- Na guia Cobertura de runtime dos clusters do EKS, você pode visualizar as estatísticas de cobertura agregadas pelo status da cobertura que está disponível na tabela Lista de clusters.
  - Você pode filtrar a tabela Lista de clusters pelas seguintes colunas:
    - Nome do cluster
    - ID da conta
    - Tipo de gerenciamento de agentes
    - Status da cobertura

    - Add-on version
- Se algum dos seus clusters do EKS tiver o Status de cobertura como Não íntegro, a coluna Problema poderá incluir informações adicionais sobre o motivo do status Não íntegro.

API/CLI

- Execute a ListCoverageAPI com seu próprio ID de detector, região e ponto de extremidade de serviço válidos. É possível filtrar e classificar a lista de clusters utilizando essa API.
    - Você pode alterar o `filter-criteria` de exemplo com uma das seguintes opções para `CriterionKey`:
        - `ACCOUNT_ID`
        - `CLUSTER_NAME`
        - `RESOURCE_TYPE`
        - `COVERAGE_STATUS`
        - `ADDON_VERSION`
        - `MANAGEMENT_TYPE`
    - Você pode alterar o `AttributeName` de exemplo em `sort-criteria` com uma das seguintes opções:
        - `ACCOUNT_ID`
        - `CLUSTER_NAME`
        - `COVERAGE_STATUS`
        - `ISSUE`
        - `ADDON_VERSION`
        - `UPDATED_AT`
    - Você pode alterar o *`max-results`* (até 50).
    - Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no https://console.aws.amazon.com/guardduty/console ou execute a ListDetectorsAPI.

```
aws guardduty --region us-east-1 list-coverage --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --sort-criteria '{"AttributeName":
 "CLUSTER_NAME", "OrderBy": "DESC"}' --filter-criteria
```

```
 '{"FilterCriterion":[{"CriterionKey":"ACCOUNT_ID", "FilterCondition":
{"EqualsValue":"111122223333"}}] }'  --max-results 5
```

- Execute a GetCoverageStatisticsAPI para recuperar estatísticas agregadas de cobertura com base no. `statisticsType`
  - Você pode alterar o `statisticsType` de exemplo com uma das seguintes opções:
    - `COUNT_BY_COVERAGE_STATUS`: representa estatísticas de cobertura para clusters do EKS agregadas por status de cobertura.
    - `COUNT_BY_RESOURCE_TYPE`— Estatísticas de cobertura agregadas com base no tipo de AWS recurso na lista.
    - Você pode alterar o `filter-criteria` de exemplo no comando. É possível usar as seguintes opções para `CriterionKey`:
      - `ACCOUNT_ID`
      - `CLUSTER_NAME`
      - `RESOURCE_TYPE`
      - `COVERAGE_STATUS`
      - `ADDON_VERSION`
      - `MANAGEMENT_TYPE`
  - Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no https://console.aws.amazon.com/guardduty/console ou execute a ListDetectorsAPI.

```
aws guardduty --region us-east-1 get-coverage-statistics --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --statistics-type COUNT_BY_COVERAGE_STATUS
 --filter-criteria '{"FilterCriterion":[{"CriterionKey":"ACCOUNT_ID",
 "FilterCondition":{"EqualsValue":"123456789012"}}] }'
```

Se o status da cobertura do seu cluster do EKS for Não íntegro, consulte Solucionando problemas de cobertura de runtime do Amazon EKS.

Alteração do status da cobertura com EventBridge notificações

O status de cobertura de um cluster do EKS em sua conta pode aparecer como Não íntegro. Para detectar quando o status da cobertura se torna Não íntegro, recomendamos que você monitore o status de cobertura periodicamente e solucione o problema, se o status for Não íntegro. Como

alternativa, você pode criar uma EventBridge regra da Amazon para notificá-lo quando o status da cobertura mudar de `Unhealthy` para `Healthy` ou não. Por padrão, GuardDuty publica isso no EventBridge barramento da sua conta.

Exemplo de esquema de notificação

Em uma EventBridge regra, você pode usar os exemplos de eventos e padrões de eventos predefinidos para receber a notificação do status da cobertura. Para obter mais informações sobre a criação de uma EventBridge regra, consulte Criar regra no Guia EventBridge do usuário da Amazon.

Além disso, você pode criar um padrão de evento personalizado usando o exemplo de esquema de notificação a seguir. Substitua os valores da sua conta. Para ser notificado quando o status da cobertura do seu cluster Amazon EKS mudar de `Healthy` para`Unhealthy`, `detail-type` deveria ser*`GuardDuty Runtime Protection Unhealthy`*. Para ser notificado quando o status da cobertura mudar de `Unhealthy` para`Healthy`, substitua o valor de `detail-type` por*`GuardDuty Runtime Protection Healthy`*.

```
{
  "version": "0",
  "id": "event ID",
  "detail-type": "GuardDuty Runtime Protection Unhealthy",
  "source": "aws.guardduty",
  "account": "Conta da AWS ID",
  "time": "event timestamp (string)",
  "region": "Região da AWS",
  "resources": [
       ],
  "detail": {
    "schemaVersion": "1.0",
    "resourceAccountId": "string",
    "currentStatus": "string",
    "previousStatus": "string",
    "resourceDetails": {
        "resourceType": "EKS",
        "eksClusterDetails": {
            "clusterName": "string",
            "availableNodes": "string",
             "desiredNodes": "string",
             "addonVersion": "string"
         }
    },
    "issue": "string",
```

```
    "lastUpdatedAt": "timestamp"
  }
}
```

Solucionando problemas de cobertura de runtime do Amazon EKS

Se o status da cobertura do seu cluster EKS for`Unhealthy`, você poderá visualizar o erro correspondente na coluna Problema no GuardDuty console ou usando o tipo de CoverageResourcedados.

Ao trabalhar com tags de inclusão ou exclusão para monitorar seus clusters do EKS seletivamente, pode levar algum tempo para que as tags sejam sincronizadas. Isso pode afetar o status de cobertura do cluster do EKS associado. É possível tentar remover e adicionar a tag correspondente (inclusão ou exclusão) novamente. Para obter mais informações, consulte Marcar os recursos do Amazon EKS no Guia do desenvolvedor do Amazon EKS.

A estrutura de um problema de cobertura é `Issue type:Extra information`. Normalmente, os problemas terão Informações adicionais opcionais que poderão incluir uma exceção específica do lado do cliente ou uma descrição sobre o problema. Com base nas Informações adicionais, as tabelas a seguir fornecem as etapas recomendadas para solucionar os problemas de cobertura para seus clusters EKS.

Tipo de problema (prefixo)	Informações adicionais	Etapas para solução de problemas
Falha na criação de complemento	O complemento não `aws-guardduty-agent` é compatível com a versão atual do cluster*`ClusterName`* . O complemento especificado é compatível.	Certifique-se de usar uma dessas versões do Kubernetes compatíveis com a implantação do complemento EKS `aws-guardduty-agent` . Para obter mais informações, consulte Versões do Kubernetes suportadas pelo agente de segurança GuardDuty. Para obter informações sobre como atualizar sua versão do Kubernetes, consulte

Tipo de problema (prefixo)	Informações adicionais	Etapas para solução de problemas
		Atualizando uma versão do Kubernetes do cluster do Amazon EKS.
Falha na criação de complemento Falha na atualização do complemento Status do complemento não íntegro	Problema no complemento do EKS - `AddonIssueCode : AddonIssueMessage`	Para obter informações sobre as etapas recomendadas para um código específico de problema do complemento, consulte Troubleshooting steps for Addon creation/ update error with Addon issue code. Para obter uma lista dos códigos de problemas adicionais que você pode enfrentar nesse problema, consulte AddonIssue.
Falha na criação de endpoint da VPC	A criação de VPC endpoint não é compatível com VPC compartilhada *vpcId*	O Monitoramento de runtime agora suporta o uso de uma VPC compartilhada em uma organização. Verifique se suas contas atendem a todos os pré-requisitos. Para obter mais informações, consulte Pré-requisitos para usar a VPC compartilhada.

Tipo de problema (prefixo)	Informações adicionais	Etapas para solução de problemas
	Somente ao usar VPC compartilhada com configuração de agente automatizado O ID da conta do *111122223333* proprietário da VPC compartilhada *vpcId* não tem o Runtime Monitoring, a configuração automatizada do agente ou ambos ativados.	A conta compartilhada do proprietário da VPC deve habilitar o Monitoramento de runtime e a configuração de agente automatizado para pelo menos um tipo de recurso (Amazon EKS ou Amazon ECS (AWS Fargate)). Para obter mais informações, consulte Pré-requisitos específicos para o monitoramento de tempo de execução GuardDuty.
	A ativação do DNS privado requer ambos `enableDnsSupport` e os atributos da `enableDnsHostnames` VPC definidos `true` como *vpcId* for (Serviço: Ec2, Code:400 Status, ID da solicitação:). *a1b2c3d4-5678-90ab-cdef-EXAMPLE11111*	Verifique se os seguintes atributos da VPC estão definidos como `true`: `enableDnsSupport` e `enableDnsHostnames`. Para obter mais informações, consulte Atributos de DNS na sua VPC. Se você estiver usando o Amazon VPC Console em https://console.aws.amazon.com/vpc/para criar o Amazon VPC, certifique-se de selecionar Habilitar nomes de host DNS e Ativar resolução de DNS. Para obter mais informações, consulte Opções de configuração da VPC.

Tipo de problema (prefixo)	Informações adicionais	Etapas para solução de problemas
Falha na exclusão de endpoint da VPC compartilhada	A exclusão compartilhada do VPC endpoint não é permitida para ID da conta, *vpcId* VPC *111122223333* compartilhada e ID da conta do proprietário. *555555555555*	Etapas possíveis: • A desativação do status de Monitoramento de runtime da conta de participante da VPC compartilhada não afeta a política de endpoint da VPC compartilhada e o grupo de segurança que existe na conta do proprietário. Para excluir o grupo de segurança e endpoint da VPC compartilhada, desative o Monitoramento de runtime ou o status de configuração de agente automatizado na conta do proprietário da VPC compartilhada. • A conta do participante da VPC compartilhada não pode excluir o grupo de segurança e o endpoint da VPC compartilhada hospedados na conta compartilhada do proprietário da VPC.

Tipo de problema (prefixo)	Informações adicionais	Etapas para solução de problemas
Clusters locais do EKS	Os complementos do EKS não são compatíveis com clusters de Outposts locais.	Não acionável. Para obter mais informaçõ es, consulte Amazon EKS em AWS postos avançados.
A permissão de habilitação do Monitoramento de runtime do EKS não foi concedida	(pode ou não mostrar informações adicionais)	1. Se houver informações adicionais disponíveis para esse problema, corrija a causa raiz e siga a próxima etapa. 2. Desative o Monitoramento de runtime do EKS e depois ative-o novamente. Certifiqu e-se de que o GuardDuty agente também seja implantado, seja de forma automática GuardDuty ou manual.
Provisionamento de recursos de habilitação do Monitoram ento de runtime do EKS em andamento	(pode ou não mostrar informações adicionais)	Não acionável. Depois de habilitar o Monitoramento de runtime do EKS, o status da cobertura pode permanecer `Unhealthy` até que a etapa de provision amento de recursos seja concluída. O status da cobertura é monitorado e atualizado periodicamente.

Tipo de problema (prefixo)	Informações adicionais	Etapas para solução de problemas
Outros (qualquer outro problema)	Erro devido a falha na autorização	Desative o Monitoramento de runtime do EKS e depois ative-o novamente. Certifique-se de que o GuardDuty agente também seja implantado, de forma automática GuardDuty ou manual.

Etapas de solução de problemas para creation/update erro do complemento com o código de problema do complemento

Erro na criação ou atualização do complemento	Etapas de solução de problemas
Problema do complemento EKS - `InsufficientNumberOfReplicas` : O complemento não está íntegro porque não tem o número desejado de réplicas.	• Usando a mensagem do problema, é possível identificar e corrigir a causa raiz. Comece descrevendo seu cluster. Por exemplo, use `kubectl describe pods` para identificar a causa raiz da falha do pod. Depois de corrigir a causa raiz, repita a etapa (criação ou atualização do complemento). • Se o problema persistir, valide se o endpoint da VPC do seu cluster Amazon EKS está corretamente configurado. Para obter mais informações, consulte Validando a configuração do endpoint da VPC.
Problema do complemento do EKS – `InsufficientNumberOfReplicas` : o complemento não está íntegro porque um ou mais pods não está programado. Os nós `0/x` estão disponíveis: `x Insufficient cpu.`	Para resolver esse problema, você pode realizar um dos seguintes procedimentos: • Atualize a prioridade do pod do GuardDuty agente: Parâmetros e valores configuráveis definindo o `PriorityClass`

Erro na criação ou atualização do complemento	Etapas de solução de problemas
`preemption: not eligible due to preemptionPolicy=Never` .	para qualquer uma das opções que suportam o `preemptionPolicy` valor como`PreemptLowerPriority` . Para obter informações sobre a prioridade do pod, consulte Prioridade de pods e preempção na Documentação do Kubernetes. • Amplie a instância: Para gerenciar seus recursos e fazer a seleção ideal de instância s, consulte Gerenciar recursos computaci onais usando nós e Escolher um tipo de instância de nó ideal do Amazon EC2 no Guia do usuário do Amazon EKS.
Problema do complemento do EKS – `InsufficientNumberOfReplicas` : o complemento não está íntegro porque um ou mais pods não está programado. Os nós `0/x` estão disponíveis: `x Too many pods. preemption: not eligible due to preemptionPolicy=Never` .	
Problema do complemento do EKS – `InsufficientNumberOfReplicas` : o complemento não está íntegro porque um ou mais pods não está programado. Os nós `0/x` estão disponíveis: `1 Insufficient memory. preemption: not eligible due to preemptionPolicy=Never` .	

> **Note**
>
> A mensagem é exibida `0/x` porque GuardDuty relata somente o primeiro erro encontrado. O número real de pods em execução no GuardDuty daemonset pode ser maior que 0.

Erro na criação ou atualização do complemento	Etapas de solução de problemas
Problema do complemento do EKS – `InsufficientNumberOfReplicas` : o complemento não está íntegro porque um ou mais pods têm contêineres de espera `CrashLoopBackOff: Completed`	Você pode ver os logs associados ao pod e identificar o problema. Para obter informações sobre como fazer isso, consulte Depurar pods em execução na Documentação do Kubernetes. Para solucionar esse problema de complemento, use esta lista de verificação: • Confirme se o Monitoramento de Runtime está habilitado. • Confirme se Pré-requisitos para o suporte ao cluster do Amazon EKS, como as distribuições de sistema operacional verificadas e as versões compatíveis do Kubernetes, foram atendidos. • Ao gerenciar o agente de segurança manualmente, confirme que você criou um endpoint da VPC para todas as VPCs. Ao habilitar a configuração GuardDuty automatizada, você ainda deve validar a criação do VPC endpoint. Por exemplo, ao usar uma VPC compartilhada em uma configuração automatizada. Para validar isso, consulte Validando a configuração do endpoint da VPC. • Confirme se o agente GuardDuty de segurança é capaz de resolver o DNS GuardDuty privado do VPC endpoint. Para conhecer os endpoints, consulte Nomes DNS privados para endpoints em Gerenciando agentes GuardDuty de segurança.

Erro na criação ou atualização do complemento	Etapas de solução de problemas
	Para fazer isso, você pode usar a ferramenta `nslookup` no Windows ou Mac ou a ferramenta `dig` no Linux. Ao usar o nslookup, você pode usar o seguinte comando depois de substituir a região pela sua região*us-west-2* : `nslookup guardduty-data. us-west-2 .amazonaws.com` • Verifique se sua política de GuardDuty VPC endpoint ou a política de controle de serviços não está afetando a ação. `guardduty :SendSecurityTelemetry`

Erro na criação ou atualização do complemento	Etapas de solução de problemas
Problema do complemento do EKS – `InsufficientNumberOfReplicas` : o complemento não está íntegro porque um ou mais pods têm contêineres de espera `CrashLoopBackOff: Error`	Você pode ver os logs associados ao pod e identificar o problema. Para obter informações sobre como fazer isso, consulte Depurar pods em execução na Documentação do Kubernetes. Depois de identificar o problema, use a lista de verificação a seguir para solucionar o problema: • Confirme se o Monitoramento de Runtime está habilitado. • Confirme se Pré-requisitos para o suporte ao cluster do Amazon EKS, como as distribuições de sistema operacional verificadas e as versões compatíveis do Kubernetes, foram atendidos. • O agente GuardDuty de segurança é capaz de resolver o DNS GuardDuty privado do VPC endpoint. Para conhecer os endpoints, consulte Nomes DNS privados para endpoints em Gerenciando agentes GuardDuty de segurança.
Problema de complemento de EKS - `AdmissionRequestDenied` : webhook de admissão `"validate.kyverno.svc-fail"` negou a solicitação: política `DaemonSet/amazon-guardduty/aws-guardduty-agent` para violação de recurso: restrict-image-registries: `autogen-validate-registries` : ...	1. O cluster do Amazon EKS ou o administrador de segurança devem revisar a política de segurança que está bloqueando a atualização do complemento. 2. Você deve desabilitar o controlador (webhook) ou fazer com que o controlador aceite as solicitações do Amazon EKS.

Erro na criação ou atualização do complemento	Etapas de solução de problemas
Problema do complemento EKS -`ConfigurationConflict` : Conflitos encontrados ao tentar aplicar. Não continuará devido ao modo de resolução de conflitos. `Conflicts: DaemonSet.apps aws-guardduty-agent - .spec.template.spec.containers[name="aws-guardduty-agent"].image`	Ao criar ou atualizar o complemento, forneça o sinalizador `OVERWRITE` de resolução de conflitos. Isso possivelmente substituirá quaisquer alterações que tenham sido feitas diretamente nos recursos relacionados no Kubernetes usando a API do Kubernetes. Primeiro, é possível Remover um complemento do Amazon EKS de um cluster e depois reinstalar.

Erro na criação ou atualização do complemento	Etapas de solução de problemas

Problema de Complemento de EKS - `AccessDenied: priorityclasses.scheduling.k8s.io "aws-guardduty-agent.priorityclass" is forbidden: User "eks:addon-manager" cannot patch resource "priorityclasses" in API group "scheduling.k8s.io" at the cluster scope`	Você deve adicionar a permissão ausente ao `eks:addon-cluster-admin ClusterRoleBinding` manualmente. Adicione o seguinte `yaml` ao `eks:addon-cluster-admin` :
	`---`
	`kind: ClusterRoleBinding`
	`apiVersion: rbac.authorization.k8s.io/v1`
	`metadata:`
	`  name: eks:addon-cluster-admin`
	`subjects:`
	`- kind: User`
	`  name: eks:addon-manager`
	`  apiGroup: rbac.authorization.k8s.io`
	`roleRef:`
	`  kind: ClusterRole`
	`  name: cluster-admin`
	`  apiGroup: rbac.authorization.k8s.io`
	`---`
	Agora você pode aplicar esse `yaml` ao cluster do Amazon EKS usando o seguinte comando:
	`kubectl apply -f eks-addon-cluster-admin.yaml`

AddonUpdationFailed: EKSAddonIssue - `AccessDenied: namespaces\"amazon-guardduty\"isforbidden:User\"eks:addon-manager\"cannotpatchresource\"namespaces\"inAPIgroup\"\"inthenamespace\"amazon-guardduty\"`	
Problema de Complemento de EKS - `AccessDenied: admission webhook "validation.gatekeeper.sh" denied the request: [all-namespace-must-have-label-owner] All namespaces must have an `owner` label`	Você deve desabilitar o controlador ou fazer com que o controlador aceite as solicitações do cluster Amazon EKS. Antes de criar ou atualizar o complemento, você também pode criar um GuardDuty namespace e rotulá-lo como. `owner`

Erro na criação ou atualização do complemento	Etapas de solução de problemas
Problema de Complemento de EKS - `AccessDenied: admission webhook "validation.gatekeeper.sh" denied the request: [allowed-container-registries] container <aws-guarddduty-agent> has an invalid image registry`	Adicione o registro de imagens GuardDuty ao `allowed-container-registries` em seu controlador de admissão. Para obter mais informações, consulte Repositório do ECR para EKS v1.8.1-eks-build.2 em Agente de hospedagem de repositórios Amazon ECR GuardDuty.

Configurar o monitoramento da CPU e da memória

Depois de habilitar o Monitoramento de runtime e avaliar se o status da cobertura do seu cluster é Íntegro, você pode configurar e visualizar as métricas do insight.

Os tópicos a seguir podem ajudá-lo a avaliar o desempenho do agente implantado em relação aos limites de CPU e memória do GuardDuty agente.

Como configurar o monitoramento no cluster do Amazon ECS

As etapas a seguir do Guia CloudWatch do usuário da Amazon podem ajudá-lo a avaliar o desempenho do agente implantado em relação aos limites de CPU e memória do GuardDuty agente:

1. Configurando o Container Insights no Amazon ECS para métricas no nível de cluster e de serviço
2. Métricas do Amazon ECS Container Insights

Configurando o monitoramento no cluster do Amazon EKS

Depois que o agente de GuardDuty segurança for implantado e você avaliar se o status da cobertura do seu cluster está íntegro, você pode configurar e visualizar as métricas do Container Insights.

Avaliar o desempenho do agente de segurança

1. Configuração do Container Insights no Amazon EKS e no Kubernetes no Guia do usuário da Amazon CloudWatch

2. Métricas do Amazon EKS e do Kubernetes Container Insights no Guia do usuário da Amazon CloudWatch

Gerenciar o desempenho com o agente de segurança v1.5.0 e superior

Com o Security Agent v1.5.0 e versões posteriores, quando os insights indicam que o GuardDuty agente associado está atingindo os limites atribuídos, você pode configurar parâmetros específicos. Para obter mais informações, consulte Configurar parâmetros do complemento do EKS.

Como usar uma VPC compartilhada com Monitoramento de Runtime

GuardDuty O Runtime Monitoring suporta o uso compartilhado da Amazon Virtual Private Cloud (Amazon VPC) para Contas da AWS aqueles que pertencem à mesma organização em. AWS OrganizationsÉ possível usar a VPC compartilhada de duas maneiras:

- Configuração automatizada do agente (recomendada) — Quando gerencia GuardDuty automaticamente o agente de segurança, ele também configura a política de endpoint do Amazon VPC. Essa política é baseada nas configurações de VPC compartilhadas da sua organização.

  Você deve habilitar a configuração automatizada do agente na conta compartilhada do proprietário da VPC e em todas as contas participantes que compartilharão essa VPC.
- Agente gerenciado manualmente – ao gerenciar manualmente o agente de segurança com a VPC compartilhada, você deve atualizar a política de endpoint da VPC para permitir que as contas correspondentes acessem a VPC compartilhada. Para fazer isso, você pode usar o exemplo de política compartilhado na seção Como funciona a seguir.

  Para cenários de gerenciamento manual envolvendo contas participantes de VPC compartilhada, o status da cobertura pode não ser preciso. Para garantir a proteção e o status de cobertura atualizados de seus recursos, GuardDuty recomenda habilitar a configuração automática de agentes para todas as contas que usarão a VPC compartilhada.

Tópicos

- Como funciona
- Pré-requisitos para usar a VPC compartilhada

Como funciona

Aqueles Contas da AWS que pertencem à mesma organização da conta compartilhada do proprietário da Amazon VPC também podem compartilhar o mesmo endpoint da Amazon VPC. Cada uma das contas que compartilham a mesma Amazon VPC é chamada de AWS conta participante da Amazon VPC compartilhada associada.

O exemplo a seguir mostra a política padrão de endpoint da VPC da conta compartilhada do proprietário da VPC e da conta do participante. `aws:PrincipalOrgID` mostrará a ID da organização associada ao recurso VPC compartilhado. O uso desta política é limitado às contas de participantes presentes na organização da conta do proprietário.

Example Exemplo de política de endpoint da VPC compartilhada

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [{
            "Action": "*",
            "Resource": "*",
            "Effect": "Allow",
            "Principal": "*"
        },
        {
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalOrgID": "o-abcdef0123"
                }
            },
            "Action": "*",
            "Resource": "*",
            "Effect": "Deny",
            "Principal": "*"
        }
    ]
}
```

Com configuração GuardDuty automática de agentes

Quando a conta do proprietário da VPC compartilhada ativa o Runtime Monitoring e a configuração automática do agente para qualquer um dos recursos (Amazon EKS ou (somente AWS Fargate Amazon ECS)), todas as VPCs compartilhadas se tornam elegíveis para a instalação automática do endpoint compartilhado da Amazon VPC e do grupo de segurança associado na conta do proprietário da VPC compartilhada. GuardDuty recupera o ID da organização que está associado à Amazon VPC compartilhada.

GuardDuty cria um endpoint da Amazon VPC quando a conta compartilhada do proprietário da VPC ou a conta participante precisam dela. Exemplos de necessidade de um endpoint Amazon VPC incluem GuardDuty habilitar, Runtime Monitoring, EKS Runtime Monitoring ou iniciar uma nova tarefa da Amazon. ECS-Fargate Quando essas contas habilitam o Runtime Monitoring e a configuração automática de agentes para qualquer tipo de recurso, GuardDuty cria um endpoint da Amazon VPC e define a política de endpoint com o mesmo ID de organização da conta compartilhada do proprietário da VPC. GuardDuty adiciona uma `GuardDutyManaged` tag e a define `true` para o endpoint da Amazon VPC que cria. GuardDuty Se a conta compartilhada do proprietário da Amazon VPC não tiver habilitado o Runtime Monitoring ou a configuração automatizada do agente para nenhum dos recursos, não GuardDuty definirá a política de endpoint da Amazon VPC. Para obter informações sobre como configurar o Monitoramento de runtime e gerenciar automaticamente o agente de segurança na conta compartilhada do proprietário da VPC, consulte Habilitando o GuardDuty monitoramento de tempo.

Uso com agente gerenciado manualmente

Ao usar a VPC compartilhada com um agente gerenciado manualmente, confirme se não há uma política de endpoint `Deny` explícita que bloqueie qualquer conta que precise usar a VPC compartilhada. Isso impede que o agente de segurança envie telemetria para GuardDuty, resultando em um status de `Unhealthy` cobertura. Para configurar a política de endpoint, consulte Example shared VPC endpoint policy.

A cobertura de runtime pode não ser precisa em cenários como a falta de permissões para a VPC compartilhada. Você pode monitorar continuamente a cobertura de recursos seguindo as etapas para seu tipo de recurso em Analisando estatísticas de cobertura de runtime e solucionando problemas.

Para garantir a proteção contínua de seus recursos computacionais pelo Runtime Monitoring, GuardDuty recomenda ativar a configuração automática do agente para a conta compartilhada do proprietário da VPC e para todas as contas participantes dos seus recursos.

Pré-requisitos para usar a VPC compartilhada

Como parte de uma configuração inicial, execute as seguintes etapas na Conta da AWS qual você deseja ser o proprietário da VPC compartilhada:

1. Criando uma organização: crie uma organização, seguindo as etapas em Criando e gerenciando uma organização no AWS Organizations Guia do usuário.

   Para obter informações sobre como adicionar ou remover contas de membros, consulte Gerenciamento Contas da AWS na sua organização.
2. Criando um recurso de VPC compartilhado — Você pode criar um recurso de VPC compartilhado a partir da conta do proprietário. Para obter mais informações, consulte Compartilhar as sub-redes da sua VPC com outras contas no Guia do usuário da Amazon VPC.

Pré-requisitos específicos para o monitoramento de tempo de execução GuardDuty

A lista a seguir fornece os pré-requisitos específicos para: GuardDuty

- A conta do proprietário da VPC compartilhada e a conta participante podem ser de diferentes organizações em. GuardDuty Contudo, elas devem pertencer à mesma organização em AWS Organizations. Isso é necessário GuardDuty para criar um endpoint da Amazon VPC e um grupo de segurança para a VPC compartilhada. Para obter informações sobre como funciona as VPCs compartilhadas, consulte Compartilhar sua VPC com outras contas no Guia do usuário Amazon VPC.
- Ative o Runtime Monitoring ou o EKS Runtime Monitoring e a configuração GuardDuty automatizada do agente para qualquer recurso na conta compartilhada do proprietário da VPC e na conta do participante. Para obter mais informações, consulte Como habilitar o monitoramento de runtime.

  Se você já concluiu essas configurações, prossiga para a próxima etapa.
- Ao trabalhar com uma tarefa do Amazon EKS ou do Amazon ECS (AWS Fargate somente), certifique-se de escolher o recurso VPC compartilhado associado à conta do proprietário e selecionar suas sub-redes.

Usando a Infraestrutura como Código (IaC) com agentes de segurança GuardDuty automatizados

Use esta seção somente se a seguinte lista se aplicar ao seu caso de uso:

- Você usa ferramentas de Infraestrutura como Código (IaC), como o Terraform, para gerenciar seus AWS recursos AWS Cloud Development Kit (AWS CDK) e
- Você precisa habilitar a configuração GuardDuty automática do agente para um ou mais tipos de recursos: Amazon EKS, Amazon EC2 ou Amazon. ECS-Fargate

Visão geral do gráfico de dependência de recursos da IaC

Quando você ativa a configuração GuardDuty automatizada do agente para um tipo de recurso, cria GuardDuty automaticamente um VPC endpoint e um grupo de segurança associados a esse VPC endpoint e instala o agente de segurança para esse tipo de recurso. Por padrão, GuardDuty excluirá o VPC endpoint e o grupo de segurança associado somente depois que você desabilitar o Runtime Monitoring. Para obter mais informações, consulte Desativação, desinstalação e remoção de recursos no Monitoramento de runtime.

Quando uma ferramenta de IaC é usada, ela mantém um gráfico de dependência dos recursos. No momento da exclusão dos recursos usando a ferramenta IaC, ela exclui apenas os recursos que podem ser rastreados como parte do gráfico de dependência dos recursos. As ferramentas IaC podem não conhecer os recursos criados fora da configuração especificada. Por exemplo, você cria uma VPC com uma ferramenta de IaC e, em seguida, adiciona um grupo de segurança a essa VPC usando o AWS console ou uma operação de API. No gráfico de dependência de recursos, o recurso da VPC criada depende do grupo de segurança associado. Ao excluir esse recurso da VPC usando a ferramenta IaC, um erro será gerado. A maneira de contornar esse erro é excluir manualmente o grupo de segurança associado ou atualizar a configuração da IaC para incluir esse recurso adicional.

Problema comum - Como excluir recursos na IaC

Ao usar a configuração GuardDuty automatizada do agente, talvez você queira excluir um recurso (Amazon EKS, Amazon EC2 ou Amazon ECS-Fargate) que você criou usando uma ferramenta IaC. No entanto, esse recurso depende de um VPC endpoint criado. GuardDuty Isso impede que a ferramenta IaC exclua o recurso sozinha e exige que você desative o Monitoramento de runtime, que exclua ainda mais o endpoint da VPC automaticamente.

Por exemplo, ao tentar excluir o VPC endpoint GuardDuty criado em seu nome, você receberá um erro semelhante aos exemplos a seguir.

Example

Exemplo de erro ao usar o CDK

```
The following resource(s) failed to delete:
 [mycdkvpcapplicationpublicsubnet1Subnet1SubnetEXAMPLE1, mycdkvpcapplicationprivatesubnet1Subne
Resource handler returned message: "The subnet 'subnet-APKAEIVFHP46CEXAMPLE' has
 dependencies and cannot be deleted. (Service: Ec2, Status Code: 400, Request
 ID: e071c3c5-7442-4489-838c-0dfc6EXAMPLE)" (RequestToken: 4381cff8-6240-208a-8357-5557b7EXAMPL
 HandlerErrorCode: InvalidRequest)
```

Example

Exemplo de erro ao usar o Terraform

```
module.vpc.aws_subnet.private[1]: Still destroying... [id=subnet-APKAEIVFHP46CEXAMPLE,
 19m50s elapsed]
module.vpc.aws_subnet.private[1]: Still destroying... [id=subnet-APKAEIVFHP46CEXAMPLE,
 20m0s elapsed]

Error: deleting EC2 Subnet (subnet-APKAEIBAERJR2EXAMPLE): DependencyViolation: The
 subnet 'subnet-APKAEIBAERJR2EXAMPLE' has dependencies and cannot be deleted.
       status code: 400, request id: e071c3c5-7442-4489-838c-0dfc6EXAMPLE
```

> **Note**
>
> A versão 6.43.0 e posterior do AWS provedor Terraform resolve esse problema automaticamente. O AWS provedor detecta e remove endpoints de GuardDuty-managed VPC e grupos de segurança durante. `terraform destroy` Essa correção se aplica a todos os tipos de recursos (Amazon EKS, Amazon EC2 e Amazon ECS-Fargate).

Solução - Evite o problema de exclusão de recursos

Esta seção ajuda você a gerenciar o VPC endpoint e o grupo de segurança, independentemente de. GuardDuty

Para obter a propriedade total dos recursos configurados usando a ferramenta IaC, execute as seguintes etapas na ordem listada:

1. Crie uma VPC. Para permitir a permissão de entrada, associe um GuardDuty VPC endpoint ao grupo de segurança a essa VPC.
2. Ative a configuração GuardDuty automática do agente para seu tipo de recurso

Depois de concluir as etapas anteriores, não GuardDuty criará seu próprio VPC endpoint e reutilizará o que você criou usando a ferramenta IaC.

Para obter informações sobre como criar sua própria VPC, consulte Criar uma VPC somente nos Gateways de trânsito da Amazon VPC. Para obter informações sobre como criar um endpoint da VPC, consulte a seção a seguir sobre o tipo de recurso:

- Para o Amazon EC2, consulte Pré-requisito — Criando um endpoint da Amazon VPC manualmente.
- Para o Amazon EKS, consulte Pré-requisito — Como criar um endpoint da VPC da Amazon.

Tipos de eventos de tempo de execução coletados que GuardDuty usam

O agente GuardDuty de segurança coleta os seguintes tipos de eventos e os envia ao GuardDuty back-end para detecção e análise de ameaças. GuardDuty não torna esses eventos acessíveis para você. Se GuardDuty detectar uma ameaça potencial e gerar umaTipos de descoberta do Monitoramento de runtime, você poderá ver os detalhes da descoberta correspondente.

Para obter informações sobre como GuardDuty usa os tipos de eventos coletados no Runtime Monitoring, consulteOptar por não usar seus dados para melhorar o serviço.

Eventos do processo

Os eventos de processo representam informações associadas aos processos em execução nas instâncias do Amazon EC2 e nos workloads de contêineres. A tabela a seguir inclui os nomes dos campos e as descrições dos eventos do processo que o Monitoramento de runtime coleta para detectar possíveis ameaças.

Nome do campo	Description
Nome do processo	Nome do processo observado.
Caminho do processo	Caminho absoluto do processo executável.
ID do processo	O ID atribuído ao processo pelo sistema operacional.
PID do namespace	O ID do processo em um namespace de PID secundário diferente do namespace de PID no nível do host. Para processos em um contêiner , é o ID do processo observado dentro do contêiner.
ID do usuário do processo	O ID exclusivo do usuário que executou o processo.
UUID do processo	A ID exclusiva atribuída ao processo por GuardDuty.
GID do processo	ID de processo do grupo de processos.
EGID do processo	ID de grupo efetivo do grupo de processos.
EUID do processo	ID de usuário efetivo do processo.
Nome de usuário do processo	O nome do usuário que executou o processo.
Hora de início do processo	A hora de criação do processo. Esse campo está no formato de string de data UTC (`2023-03-22T19:37:20.168Z`).
Processo executável SHA-256	O hash `SHA256` do executável do processo.
Caminho do script de processo	Caminho do arquivo de script que foi executado .

Nome do campo	Description
Variável de ambiente do processo	A variável de ambiente disponibilizada para o processo. Somente `LD_PRELOAD` e `LD_LIBRARY_PATH` são coletados.
Present Working Directory (PWD – Diretório de trabalho presente) do processo	Diretório de trabalho presente do processo.
Processo pai	Detalhes do processo pai. Um processo pai é um processo que criou o processo observado.
Argumentos de linha de comando Atualmente, esse campo se limita a versões específicas do agente que correspondem ao tipo de recurso: • Fargate (somente Amazon ECS) com agente de GuardDuty segurança v1.0.0 e superior. • Instâncias do Amazon EC2 com agente de GuardDuty segurança v1.0.0 e superior. • Clusters do Amazon EKS com agente de segurança v1.4.0 e superior. Para obter mais informações, consulte GuardDuty versões de lançamento do agente de segurança.	Command-line argumentos fornecidos no momento da execução do processo. Esse campo pode conter dados confidenciais do cliente.

Eventos de contêineres

Os eventos do contêiner representam informações associadas às atividades dos workloads do contêiner. A tabela a seguir inclui os nomes de campo e as descrições dos eventos do workload de contêiner que o Monitoramento de runtime coleta para detectar ameaças em potencial.

Nome do campo	Description
Nome do contêiner	O nome do contêiner. Quando disponível, esse campo exibe o valor do rótulo `io.kubenetes.container.name` .
UID do contêiner	O ID exclusivo do contêiner atribuído pelo runtime do contêiner.
Runtime do contêiner	O runtime do contêiner (como `docker` ou `containerd`) usado para executar o contêiner.
ID da imagem do contêiner	O ID da imagem do contêiner.
Nome da imagem do contêiner	O nome da imagem do contêiner.

AWS Fargate Eventos de tarefas (somente Amazon ECS)

Fargate-Amazon Os eventos de tarefas do ECS representam atividades associadas às tarefas do Amazon ECS executadas em computadores Fargate. A tabela a seguir inclui os nomes dos campos e as descrições dos eventos de ECS-Fargate tarefas da Amazon que o Runtime Monitoring coleta para detectar possíveis ameaças.

Nome do campo	Description
Nome de recurso da Amazon (ARN) da tarefa	O ARN da tarefa.
Nome do cluster	O nome do cluster do Amazon ECS.
Nome de família	O nome de família da definição da tarefa. O `family` é usado como um nome para a definição da tarefa usada para iniciar a tarefa.
Nome do serviço	O nome do serviço do Amazon ECS, se a tarefa foi iniciada como parte de um serviço.
Tipo de inicialização	A infraestrutura na qual sua tarefa é executada. Para o Monitoramento de runtime com o tipo de recurso

Nome do campo	Description
	como`ECSCluster` , o tipo de lançamento pode ser `EC2` ou `FARGATE`.
CPU	O número de unidades de CPU usadas pela tarefa, conforme expresso na definição da tarefa.

Eventos de pod do Kubernetes

A tabela a seguir inclui os nomes dos campos e as descrições dos eventos de pod do Kubernetes que o Monitoramento de runtime coleta para detectar possíveis ameaças.

Nome do campo	Description
ID do pod	O ID do pod do Kubernetes.
Nome do pod	Nome do pod do Kubernetes.
Namespace do pod	Nome do namespace do Kubernetes ao qual a workload do Kubernetes pertence.
Nome do cluster do Kubernetes	Nome do cluster do Kubernetes.

Eventos do Sistema de Nomes de Domínio (DNS)

Os eventos do Sistema de Nomes de Domínio (DNS) incluem detalhes das consultas ao DNS feitas por seus tipos de recursos e respostas correspondentes. A tabela a seguir inclui os nomes dos campos e as descrições dos eventos DNS que o Monitoramento de runtime coleta para detectar possíveis ameaças.

Nome do campo	Description
Tipo de soquete	Tipo de soquete para indicar a semântica de comunicação. Por exemplo, `.SOCK_RAW`

Nome do campo	Description
Família de endereços	Representa o protocolo de comunicação associado ao endereço. Por exemplo, a família de endereços `AF_INET` é usada para o protocolo IPv4.
ID de direção	O ID de direção da conexão.
Número do protocolo	O número do protocolo da camada 4, como 17 para UDP e 6 para TCP.
IP de endpoint remoto de DNS	O IP remoto da conexão.
Porta de endpoint remoto de DNS	O número da porta da conexão.
IP do endpoint local de DNS	O IP local da conexão.
Porta do endpoint local de DNS	O número da porta da conexão.
Carga útil de DNS	A carga útil dos pacotes DNS que contém consultas e respostas de DNS.

Eventos abertos

Os eventos abertos estão associados ao acesso e modificação do arquivo. A tabela a seguir inclui os nomes dos campos e as descrições dos eventos abertos que o Monitoramento de runtime coleta para detectar possíveis ameaças.

Nome do campo	Description
Caminho de arquivo	Caminho de arquivo que é aberto nesse evento.
Sinalizadores	Descreve o modo de acesso ao arquivo, como somente de leitura, somente de gravação e de leitura-gravação.

Evento do módulo de carga

A tabela a seguir inclui o nome do campo e a descrição do evento de módulo de carga que o Monitoramento de runtime coleta para detectar possíveis ameaças.

Nome do campo	Description
Nome do módulo	Nome do módulo carregado no kernel.

Eventos do Mprotect

Os eventos Mprotect fornecem informações sobre alterações nas configurações de proteção de memória dos processos em execução nos sistemas monitorados. A tabela a seguir inclui os nomes dos campos e as descrições dos eventos Mprotect que o Monitoramento de runtime coleta para detectar possíveis ameaças.

Nome do campo	Description
Intervalo de endereços	O intervalo de endereços para o qual as proteções de acesso foram modificadas.
Regiões da memória	Especifica a região do espaço de endereço de um processo, como pilha e pilha.
Sinalizadores	Representa as opções que controlam o comportamento desse evento.

Eventos de montagem

Os eventos de montagem fornecem informações associadas à montagem e desmontagem de sistemas de arquivos em seu recurso monitorado. A tabela a seguir inclui os nomes dos campos e as descrições dos eventos de montagem que o Monitoramento de runtime coleta para detectar possíveis ameaças.

Nome do campo	Description
Destino de montagem	O caminho em que a origem de montagem está montada.
Fonte de montagem	O caminho no host que está montado no destino de montagem.
Tipo do sistema de arquivos	Representa o tipo de sistema de arquivos montado.
Sinalizadores	Representa as opções que controlam o comportamento desse evento.

Eventos de links

Os eventos de link fornecem visibilidade das atividades de gerenciamento de links do sistema de arquivos em seus recursos monitorados. A tabela a seguir inclui os nomes dos campos e as descrições dos eventos de link que o Monitoramento de runtime coleta para detectar possíveis ameaças.

Nome do campo	Description
Caminho do link	O caminho em que o link físico é criado.
Caminho de destino	O caminho do arquivo para o qual o link físico aponta.

Eventos do Symlink

Os eventos do Symlink fornecem visibilidade das atividades de gerenciamento de link simbólico do sistema de arquivos em seus recursos monitorados. A tabela a seguir inclui os nomes dos campos e as descrições dos eventos do symlink que o Monitoramento de runtime coleta para detectar possíveis ameaças.

Nome do campo	Description
Caminho do link	Caminho em que o link simbólico é criado.
Caminho de destino	Caminho do arquivo para o qual o link simbólico aponta.

Eventos Dup

Os eventos Dup fornecem visibilidade da duplicação de descritores de arquivos por processos executados nos recursos monitorados. A tabela a seguir inclui os nomes dos campos e as descrições dos eventos dup que o Monitoramento de runtime coleta para detectar possíveis ameaças.

Nome do campo	Description
Antigo descritor de arquivo	Um descritor de arquivo que representa um objeto de arquivo aberto.
Novo descritor de arquivo	Um novo descritor de arquivo que é uma duplicata do antigo descritor de arquivo. Os antigos e novos descritores de arquivo representam o mesmo objeto de arquivo aberto.
IP de endpoint remoto de Dup	O endereço IP remoto do soquete de rede representado pelo antigo descritor de arquivo. Aplicável somente quando o antigo descritor de arquivo representa um soquete de rede.
Porta de endpoint remoto de Dup	A porta remota do soquete de rede representado pelo antigo descritor de arquivo. Aplicável somente quando o antigo descritor de arquivo representa um soquete de rede.
IP do endpoint local de Dup	O endereço IP local do soquete de rede representado pelo antigo descritor de arquivo. Aplicável somente quando o antigo descritor de arquivo representa um soquete de rede.
Porta do endpoint local de Dup	A porta local do soquete de rede representado pelo antigo descritor de arquivo. Aplicável somente quando o antigo descritor de arquivo representa um soquete de rede.

Evento do mapa de memória

A tabela a seguir inclui o nome do campo e a descrição de eventos de mapa de memória que o Monitoramento de runtime coleta para detectar possíveis ameaças.

Nome do campo	Description
Caminho de arquivo	Caminho de arquivo para o qual a memória está mapeada.

Eventos de soquete

Os eventos de soquete fornecem informações sobre as conexões de soquete da rede usadas nas atividades dos recursos monitorados. A tabela a seguir inclui os nomes dos campos e as descrições dos eventos do soquete que o Monitoramento de runtime coleta para detectar possíveis ameaças.

Nome do campo	Description
Família de endereços	Representa o protocolo de comunicação associado ao endereço. Por exemplo, a família de endereços `AF_INET` é usada para o protocolo IPv4.
Tipo de soquete	Tipo de soquete para indicar a semântica de comunicação. Por exemplo, `.SOCK_RAW`
Número do protocolo	Especifica um protocolo específico dentro da família de endereços. Geralmente, há um único protocolo nas famílias de endereços. Por exemplo, a família de endereços `AF_INET` só tem o protocolo IP.

Eventos de conexão

Os eventos de conexão fornecem visibilidade das conexões de rede estabelecidas pelos processos em seus recursos monitorados. A tabela a seguir inclui os nomes dos campos e as descrições dos eventos de conexão que o Monitoramento de runtime coleta para detectar possíveis ameaças.

Nome do campo	Description
Família de endereços	Representa o protocolo de comunicação associado ao endereço. Por exemplo, a família de endereços `AF_INET` é usada para o protocolo IPv4.

Nome do campo	Description
Tipo de soquete	Tipo de soquete para indicar a semântica de comunicação. Por exemplo, .`SOCK_RAW`
Número do protocolo	Especifica um protocolo específico dentro da família de endereços. Geralmente, há um único protocolo nas famílias de endereços. Por exemplo, a família de endereços `AF_INET` só tem o protocolo IP.
Caminho de arquivo	Caminho do arquivo de soquete se a família de endereços for `AF_UNIX`.
IP de endpoint remoto	O IP remoto da conexão.
Porta de endpoint remoto	O número da porta da conexão.
IP do endpoint local	O IP local da conexão.
Porta do endpoint local	O número da porta da conexão.

Processar eventos Readv da VM

Os eventos de processo readv da VM fornecem visibilidade para operações de leitura realizadas pelos processos em suas próprias regiões de memória virtual. A tabela a seguir inclui os nomes dos campos e as descrições dos eventos VM readv do processo que o Monitoramento de runtime coleta para detectar possíveis ameaças.

Nome do campo	Description
Sinalizadores	Representa as opções que controlam o comportamento desse evento.
PID de destino	ID de processo do qual a memória está sendo lida.
UUID do processo de destino	O ID exclusivo do processo de destino.

Nome do campo	Description
Caminho executável de destino	Caminho absoluto do arquivo executável do processo de destino.

Processar eventos Writev da VM

Os eventos de processo writev da VM fornecem visibilidade para operações de gravação realizadas pelos processos em suas próprias regiões de memória virtual. A tabela a seguir inclui os nomes dos campos e as descrições dos eventos VM writev do processo que o Monitoramento de runtime coleta para detectar possíveis ameaças.

Nome do campo	Description
Sinalizadores	Representa as opções que controlam o comportamento desse evento.
PID de destino	ID de processo no qual a memória está sendo gravada.
UUID do processo de destino	O ID exclusivo do processo de destino.
Caminho executável de destino	Caminho absoluto do arquivo executável do processo de destino.

Eventos de rastreio de processo (Ptrace)

A chamada do sistema de rastreio de processo (Ptrace) é um mecanismo de depuração e rastreamento que permite que um processo (tracer) observe e controle a execução de outro processo (tracee). Isso fornece ao rastreador a capacidade de inspecionar e modificar memória, registros e fluxo de execução do processo de destino.

Os eventos Ptrace fornecem visibilidade do uso da chamada do sistema ptrace pelos processos executados nos recursos monitorados. A tabela a seguir inclui os nomes dos campos e as descrições dos eventos ptrace que o Monitoramento de runtime coleta para detectar possíveis ameaças.

Nome do campo	Description
PID de destino	ID de processo do processo de destino.
UUID do processo de destino	O ID exclusivo do processo de destino.
Caminho executável de destino	Caminho absoluto do arquivo executável do processo de destino.
Sinalizadores	Representa as opções que controlam o comportamento desse evento.

Vincular eventos

Os eventos de vinculação fornecem visibilidade da vinculação de soquetes da rede por processos executados nos recursos monitorados. A tabela a seguir inclui os nomes dos campos e as descrições dos eventos de vinculação que o Monitoramento de runtime coleta para detectar possíveis ameaças.

Nome do campo	Description
Família de endereços	Representa o protocolo de comunicação associado ao endereço. Por exemplo, a família de endereços `AF_INET` é usada para o protocolo IPv4.
Tipo de soquete	Tipo de soquete para indicar a semântica de comunicação. Por exemplo, .`SOCK_RAW`
Número do protocolo	O número do protocolo da camada 4, como 17 para UDP e 6 para TCP.
IP do endpoint local	O IP local da conexão.
Porta do endpoint local	O número da porta da conexão.

Eventos de escuta

Os eventos de recepção fornecem visibilidade do estado de recepção dos soquetes de rede, indicando se um soquete de rede está pronto ou não para aceitar conexões de entrada. Um processo executado em seu recurso monitorado define o soquete de rede para um estado de recepção. A tabela a seguir inclui os nomes dos campos e as descrições dos eventos de escuta que o Monitoramento de runtime coleta para detectar possíveis ameaças.

Nome do campo	Description
Família de endereços	Representa o protocolo de comunicação associado ao endereço. Por exemplo, a família de endereços `AF_INET` é usada para o protocolo IPv4.
Tipo de soquete	Tipo de soquete para indicar a semântica de comunicação. Por exemplo, .`SOCK_RAW`
Número do protocolo	O número do protocolo da camada 4, como 17 para UDP e 6 para TCP.
IP do endpoint local	O IP local da conexão.
Porta do endpoint local	O número da porta da conexão.

Eventos de renomeação

Os eventos de renomeação fornecem informações sobre a renomeação de arquivos e diretórios por processos executados nos recursos monitorados. A tabela a seguir inclui os nomes dos campos e as descrições dos eventos de renomeação que o Monitoramento de runtime coleta para detectar possíveis ameaças.

Nome do campo	Description
Caminho de arquivo	Caminho do arquivo que foi renomeado.
Destino	O novo caminho do arquivo.

Eventos Definir ID de usuário (UID)

Os eventos Definir ID de usuário (UID) fornecem visibilidade das alterações feitas na ID do usuário (UID) associada aos processos em execução nos recursos monitorados. A tabela a seguir inclui os nomes dos campos e as descrições dos eventos de UID definidas que o Monitoramento de runtime coleta para detectar possíveis ameaças.

Nome do campo	Description
Nova EUID	A nova ID de usuário efetiva do processo.
Nova UID	A nova ID de usuário do processo.

Eventos Chmod

Os eventos Chmod fornecem visibilidade para mudanças nas permissões (modo) de arquivos e diretórios nos recursos monitorados. A tabela a seguir inclui os nomes dos campos e as descrições dos eventos chmod que o Monitoramento de runtime coleta para detectar possíveis ameaças.

Nome do campo	Description
Caminho de arquivo	Caminho do arquivo que invoca esse evento.
Modo do arquivo	As permissões de acesso atualizadas para o arquivo associado.

Agente de hospedagem de repositórios Amazon ECR GuardDuty

As seções a seguir listam os repositórios do Amazon Elastic Container Registry (Amazon ECR) GuardDuty onde hospeda o agente de segurança que é implantado em seus recursos do Amazon EKS, Amazon ECS e ECS-Amazon Amazon EC2 Bottlerocket.

O pré-requisito para Pré-requisitos para acesso à imagem do contêiner requer que você forneça uma função de execução de tarefa que tenha certas permissões Amazon Elastic Container Registry (Amazon ECR). Para restringir ainda mais essas permissões, você pode adicionar o URI do repositório Amazon ECR que hospeda o GuardDuty agente para recursos do Fargate-Amazon ECS.

Conteúdo

- Repositório ECR para as versões 1.16.0 - 1.8.1 do agente EKS (eks.build.2)
- Repositório ECR para o agente EKS versão 1.8.1 (eks.build.1)
- Repositório ECR para agente em GuardDuty AWS Fargate (Somente Amazon ECS)
- Repositório ECR para GuardDuty agente em Bottlerocket ECS-EC2

Repositório ECR para as versões 1.16.0 - 1.8.1 do agente EKS (eks.build.2)

Quando você habilita a configuração GuardDuty automatizada do Runtime Monitoring for EKS, GuardDuty implantará essa versão do agente em seus clusters do Amazon EKS. Para obter informações sobre como habilitar o agente automatizado, consulte Gerenciando automaticamente o agente de segurança para recursos do Amazon EKS.

A tabela a seguir mostra os URIs do repositório Amazon ECR em que as versões do agente GuardDuty de segurança`1.16.0.eks.build.2`,,, `1.15.0.eks.build.2` `1.11.0.eks.build.2` `1.10.0.eks.build.21.9.0.eks.build.2`, e para o `1.8.0.eks.build.2` Amazon EKS estão hospedadas.

Região da AWS	URI do repositório do Amazon ECR
Oeste dos EUA (Oregon)	`602401143452.dkr.ecr.us-west-2.amazonaws.com`
	`039403964562.dkr.ecr.us-west-2.amazonaws.com`
Europa (Paris)	`602401143452.dkr.ecr.eu-west-3.amazonaws.com`
	`113643092156.dkr.ecr.eu-west-3.amazonaws.com`
Ásia-Pacífico (Mumbai)	`602401143452.dkr.ecr.ap-south-1.amazonaws.com`
	`610108029387.dkr.ecr.ap-south-1.amazonaws.com`

Região da AWS	URI do repositório do Amazon ECR
Ásia-Pacífico (Hyderabad)	900889452093.dkr.ecr.ap-south-2.amazonaws.com
	618745550137.dkr.ecr.ap-south-2.amazonaws.com
Canadá (Central)	602401143452.dkr.ecr.ca-central-1.amazonaws.com
	001188825231.dkr.ecr.ca-central-1.amazonaws.com
Oeste do Canadá (Calgary)	761377655185.dkr.ecr.ca-west-1.amazonaws.com
	–
Oriente Médio (Emirados Árabes Unidos)	759879836304.dkr.ecr.me-central-1.amazonaws.com
	601769779514.dkr.ecr.me-central-1.amazonaws.com
Europa (Londres)	602401143452.dkr.ecr.eu-west-2.amazonaws.com
	109118265657.dkr.ecr.eu-west-2.amazonaws.com
Oeste dos EUA (N. da Califórnia)	602401143452.dkr.ecr.us-west-1.amazonaws.com
	373421517865.dkr.ecr.us-west-1.amazonaws.com
Leste dos EUA (Norte da Virgínia)	602401143452.dkr.ecr.us-east-1.amazonaws.com

Região da AWS	URI do repositório do Amazon ECR
	031903291036.dkr.ecr.us-east-1.amazonaws.com
Leste dos EUA (Ohio)	602401143452.dkr.ecr.us-east-2.amazonaws.com
	591382732059.dkr.ecr.us-east-2.amazonaws.com
Europa (Irlanda)	602401143452.dkr.ecr.eu-west-1.amazonaws.com
	673884943994.dkr.ecr.eu-west-1.amazonaws.com
América do Sul (São Paulo)	602401143452.dkr.ecr.sa-east-1.amazonaws.com
	941219317354.dkr.ecr.sa-east-1.amazonaws.com
Europa (Estocolmo)	602401143452.dkr.ecr.eu-north-1.amazonaws.com
	366771026645.dkr.ecr.eu-north-1.amazonaws.com
Europa (Frankfurt)	602401143452.dkr.ecr.eu-central-1.amazonaws.com
	409493279830.dkr.ecr.eu-central-1.amazonaws.com
Europa (Zurique)	900612956339.dkr.ecr.eu-central-2.amazonaws.com
	718440343717.dkr.ecr.eu-central-2.amazonaws.com

Região da AWS	URI do repositório do Amazon ECR
Ásia-Pacífico (Singapura)	602401143452.dkr.ecr.ap-southeast-1.amazonaws.com
	584580519942.dkr.ecr.ap-southeast-1.amazonaws.com
Ásia-Pacífico (Sydney)	602401143452.dkr.ecr.ap-southeast-2.amazonaws.com
	011662287384.dkr.ecr.ap-southeast-2.amazonaws.com
Ásia-Pacífico (Jacarta)	296578399912.dkr.ecr.ap-southeast-3.amazonaws.com
	617474730032.dkr.ecr.ap-southeast-3.amazonaws.com
Ásia-Pacífico (Tóquio)	602401143452.dkr.ecr.ap-northeast-1.amazonaws.com
	781592569369.dkr.ecr.ap-northeast-1.amazonaws.com
Ásia-Pacífico (Seul)	602401143452.dkr.ecr.ap-northeast-2.amazonaws.com
	732248494576.dkr.ecr.ap-northeast-2.amazonaws.com
Asia Pacific (Osaka)	602401143452.dkr.ecr.ap-northeast-3.amazonaws.com
	810724417379.dkr.ecr.ap-northeast-3.amazonaws.com
Ásia-Pacífico (Hong Kong)	800184023465.dkr.ecr.ap-east-1.amazonaws.com

Região da AWS	URI do repositório do Amazon ECR
	790429075973.dkr.ecr.ap-east-1.amazonaws.com
Oriente Médio (Bahrein)	558608220178.dkr.ecr.me-south-1.amazonaws.com
	541829937850.dkr.ecr.me-south-1.amazonaws.com
Europa (Milão)	590381155156.dkr.ecr.eu-south-1.amazonaws.com
	528450769569.dkr.ecr.eu-south-1.amazonaws.com
Europa (Espanha)	455263428931.dkr.ecr.eu-south-2.amazonaws.com
	531047660167.dkr.ecr.eu-south-2.amazonaws.com
África (Cidade do Cabo)	877085696533.dkr.ecr.af-south-1.amazonaws.com
	379032919888.dkr.ecr.af-south-1.amazonaws.com
Ásia-Pacífico (Melbourne)	491585149902.dkr.ecr.ap-southeast-4.amazonaws.com
	750462861327.dkr.ecr.ap-southeast-4.amazonaws.com
Israel (Tel Aviv)	066635153087.dkr.ecr.il-central-1.amazonaws.com
	292660727137.dkr.ecr.il-central-1.amazonaws.com

Região da AWS	URI do repositório do Amazon ECR
Ásia-Pacífico (Malásia)	`151610086707.dkr.ecr.ap-southeast-5.amazonaws.com`
Ásia-Pacífico (Tailândia)	`121268973566.dkr.ecr.ap-southeast-7.amazonaws.com`
México (Centro)	`730335286997.dkr.ecr.mx-central-1.amazonaws.com`
Ásia-Pacífico (Taipei)	`533267051163.dkr.ecr.ap-east-2.amazonaws.com`

Repositório ECR para o agente EKS versão 1.8.1 (eks.build.1)

Esta seção fornece o repositório do Amazon ECR para o agente do Amazon EKS versão 1.8.1 (v1.8.1-eks-build.1). Se você estiver usando a versão v1.8.1-eks-build.1, GuardDuty recomenda mudar para a versão padrão do agente, que geralmente é a versão mais recente do agente. Para fazer isso, identifique o agente mais recente a partir de Versões de agente lançadas para recursos do Amazon EKS e execute as etapas em Atualização manual do agente de segurança para recursos do Amazon EKS.

A tabela a seguir mostra os URIs do repositório Amazon ECR em que a versão do agente GuardDuty de segurança do `1.8.1-eks-build.1` Amazon EKS está hospedada.

Região da AWS	URI do repositório do Amazon ECR
Oeste dos EUA (Oregon)	`039403964562.dkr.ecr.us-west-2.amazonaws.com`
Europa (Paris)	`113643092156.dkr.ecr.eu-west-3.amazonaws.com`
Ásia-Pacífico (Mumbai)	`610108029387.dkr.ecr.ap-south-1.amazonaws.com`

Região da AWS	URI do repositório do Amazon ECR
Ásia-Pacífico (Hyderabad)	`618745550137.dkr.ecr.ap-south-2.amazonaws.com`
Canadá (Central)	`001188825231.dkr.ecr.ca-central-1.amazonaws.com`
Oriente Médio (Emirados Árabes Unidos)	`601769779514.dkr.ecr.me-central-1.amazonaws.com`
Europa (Londres)	`109118265657.dkr.ecr.eu-west-2.amazonaws.com`
Oeste dos EUA (N. da Califórnia)	`373421517865.dkr.ecr.us-west-1.amazonaws.com`
Leste dos EUA (Norte da Virgínia)	`031903291036.dkr.ecr.us-east-1.amazonaws.com`
Leste dos EUA (Ohio)	`591382732059.dkr.ecr.us-east-2.amazonaws.com`
Europa (Irlanda)	`673884943994.dkr.ecr.eu-west-1.amazonaws.com`
América do Sul (São Paulo)	`941219317354.dkr.ecr.sa-east-1.amazonaws.com`
Europa (Estocolmo)	`366771026645.dkr.ecr.eu-north-1.amazonaws.com`
Europa (Frankfurt)	`409493279830.dkr.ecr.eu-central-1.amazonaws.com`
Europa (Zurique)	`718440343717.dkr.ecr.eu-central-2.amazonaws.com`
Ásia-Pacífico (Singapura)	`584580519942.dkr.ecr.ap-southeast-1.amazonaws.com`

Região da AWS	URI do repositório do Amazon ECR
Ásia-Pacífico (Sydney)	`011662287384.dkr.ecr.ap-southeast-2.amazonaws.com`
Ásia-Pacífico (Jacarta)	`617474730032.dkr.ecr.ap-southeast-3.amazonaws.com`
Ásia-Pacífico (Tóquio)	`781592569369.dkr.ecr.ap-northeast-1.amazonaws.com`
Ásia-Pacífico (Seul)	`732248494576.dkr.ecr.ap-northeast-2.amazonaws.com`
Asia Pacific (Osaka)	`810724417379.dkr.ecr.ap-northeast-3.amazonaws.com`
Ásia-Pacífico (Hong Kong)	`790429075973.dkr.ecr.ap-east-1.amazonaws.com`
Oriente Médio (Bahrein)	`541829937850.dkr.ecr.me-south-1.amazonaws.com`
Europa (Milão)	`528450769569.dkr.ecr.eu-south-1.amazonaws.com`
Europa (Espanha)	`531047660167.dkr.ecr.eu-south-2.amazonaws.com`
África (Cidade do Cabo)	`379032919888.dkr.ecr.af-south-1.amazonaws.com`
Ásia-Pacífico (Melbourne)	`750462861327.dkr.ecr.ap-southeast-4.amazonaws.com`
Israel (Tel Aviv)	`292660727137.dkr.ecr.il-central-1.amazonaws.com`

Repositório ECR para agente em GuardDuty AWS Fargate (Somente Amazon ECS)

Como pré-requisito para usar o Runtime Monitoring para a Amazon ECS-Fargate, você deve. Pré-requisitos para acesso à imagem do contêiner A imagem do contêiner auxiliar do GuardDuty agente é armazenada no Amazon ECR, com suas camadas de imagem armazenadas no Amazon S3. Para obter mais informações, consulte Implantação do agente de segurança no Amazon ECS no Fargate.

A tabela a seguir mostra os repositórios do Amazon ECR que hospedam o GuardDuty agente (somente AWS Fargate Amazon ECS) para cada um. Região da AWS

Região da AWS	URI do repositório do Amazon ECR
Oeste dos EUA (Oregon)	`733349766148.dkr.ecr.us-west-2.amazonaws.com/aws-guardduty-agent-fargate`
Europa (Paris)	`665651866788.dkr.ecr.eu-west-3.amazonaws.com/aws-guardduty-agent-fargate`
Ásia-Pacífico (Mumbai)	`251508486986.dkr.ecr.ap-south-1.amazonaws.com/aws-guardduty-agent-fargate`
Ásia-Pacífico (Hyderabad)	`950823858135.dkr.ecr.ap-south-2.amazonaws.com/aws-guardduty-agent-fargate`
Canadá (Central)	`354763396469.dkr.ecr.ca-central-1.amazonaws.com/aws-guardduty-agent-fargate`
Oriente Médio (Emirados Árabes Unidos)	`000014521398.dkr.ecr.me-central-1.amazonaws.com/aws-guardduty-agent-fargate`

Região da AWS	URI do repositório do Amazon ECR
Europa (Londres)	`892757235363.dkr.ecr.eu-west-2.amazonaws.com/aws-guardduty-agent-fargate`
Oeste dos EUA (N. da Califórnia)	`684579721401.dkr.ecr.us-west-1.amazonaws.com/aws-guardduty-agent-fargate`
Leste dos EUA (Norte da Virgínia)	`593207742271.dkr.ecr.us-east-1.amazonaws.com/aws-guardduty-agent-fargate`
Leste dos EUA (Ohio)	`307168627858.dkr.ecr.us-east-2.amazonaws.com/aws-guardduty-agent-fargate`
Europa (Irlanda)	`694911143906.dkr.ecr.eu-west-1.amazonaws.com/aws-guardduty-agent-fargate`
América do Sul (São Paulo)	`758426053663.dkr.ecr.sa-east-1.amazonaws.com/aws-guardduty-agent-fargate`
Europa (Estocolmo)	`591436053604.dkr.ecr.eu-north-1.amazonaws.com/aws-guardduty-agent-fargate`
Europa (Frankfurt)	`323658145986.dkr.ecr.eu-central-1.amazonaws.com/aws-guardduty-agent-fargate`
Europa (Zurique)	`529164026651.dkr.ecr.eu-central-2.amazonaws.com/aws-guardduty-agent-fargate`

Região da AWS	URI do repositório do Amazon ECR
Ásia-Pacífico (Singapura)	`174946120834.dkr.ecr.ap-southeast-1.amazonaws.com/aws-guardduty-agent-fargate`
Ásia-Pacífico (Sydney)	`005257825471.dkr.ecr.ap-southeast-2.amazonaws.com/aws-guardduty-agent-fargate`
Ásia-Pacífico (Jacarta)	`510637619217.dkr.ecr.ap-southeast-3.amazonaws.com/aws-guardduty-agent-fargate`
Ásia-Pacífico (Tóquio)	`533107202818.dkr.ecr.ap-northeast-1.amazonaws.com/aws-guardduty-agent-fargate`
Ásia-Pacífico (Seul)	`914738172881.dkr.ecr.ap-northeast-2.amazonaws.com/aws-guardduty-agent-fargate`
Asia Pacific (Osaka)	`273192626886.dkr.ecr.ap-northeast-3.amazonaws.com/aws-guardduty-agent-fargate`
Ásia-Pacífico (Hong Kong)	`258348409381.dkr.ecr.ap-east-1.amazonaws.com/aws-guardduty-agent-fargate`
Oriente Médio (Bahrein)	`536382113932.dkr.ecr.me-south-1.amazonaws.com/aws-guardduty-agent-fargate`
Europa (Milão)	`266869475730.dkr.ecr.eu-south-1.amazonaws.com/aws-guardduty-agent-fargate`

Região da AWS	URI do repositório do Amazon ECR
Europa (Espanha)	`919611009337.dkr.ecr.eu-south-2.amazonaws.com/aws-guardduty-agent-fargate`
África (Cidade do Cabo)	`197869348890.dkr.ecr.af-south-1.amazonaws.com/aws-guardduty-agent-fargate`
Ásia-Pacífico (Melbourne)	`251357961535.dkr.ecr.ap-southeast-4.amazonaws.com/aws-guardduty-agent-fargate`
Israel (Tel Aviv)	`870907303882.dkr.ecr.il-central-1.amazonaws.com/aws-guardduty-agent-fargate`
Ásia-Pacífico (Malásia)	`156041399949.dkr.ecr.ap-southeast-5.amazonaws.com/aws-guardduty-agent-fargate`
Ásia-Pacífico (Tailândia)	`054037130133.dkr.ecr.ap-southeast-7.amazonaws.com/aws-guardduty-agent-fargate`
Oeste do Canadá (Calgary)	`339712888787.dkr.ecr.ca-west-1.amazonaws.com/aws-guardduty-agent-fargate`
México (Centro)	`311141559934.dkr.ecr.mx-central-1.amazonaws.com/aws-guardduty-agent-fargate`
Ásia-Pacífico (Taipei)	`259886477082.dkr.ecr.ap-east-2.amazonaws.com/aws-guardduty-agent-fargate`

Repositório ECR para GuardDuty agente em Bottlerocket ECS-EC2

Nas instâncias do ECS-Amazon Amazon EC2 da Bottlerocket, GuardDuty o agente de segurança é executado como um contêiner hospedeiro. A imagem do contêiner do agente está hospedada no Amazon ECR. Para obter informações sobre os pré-requisitos, incluindo conectividade de rede e permissões necessárias do IAM, consulte. Pré-requisitos para o suporte do Bottlerocket ECS-EC2 O perfil da instância deve incluir as políticas `AmazonEC2ContainerRegistryReadOnly` gerenciadas `AmazonSSMManagedInstanceCore` e as políticas.

A tabela a seguir mostra os repositórios do Amazon ECR que hospedam o GuardDuty agente para as instâncias do Amazon ECS-Amazon EC2 Bottlerocket para cada um. Região da AWS

Região da AWS	URI do repositório do Amazon ECR
Leste dos EUA (Norte da Virgínia)	`593207742271.dkr.ecr.us-east-1.amazonaws.com/aws-guardduty-agent-ecs-ec2`
Leste dos EUA (Ohio)	`307168627858.dkr.ecr.us-east-2.amazonaws.com/aws-guardduty-agent-ecs-ec2`
Oeste dos EUA (N. da Califórnia)	`684579721401.dkr.ecr.us-west-1.amazonaws.com/aws-guardduty-agent-ecs-ec2`
US West (Oregon)	`733349766148.dkr.ecr.us-west-2.amazonaws.com/aws-guardduty-agent-ecs-ec2`
Europa (Irlanda)	`694911143906.dkr.ecr.eu-west-1.amazonaws.com/aws-guardduty-agent-ecs-ec2`
Europa (Londres)	`892757235363.dkr.ecr.eu-west-2.amazonaws.com/aws-guardduty-agent-ecs-ec2`

Região da AWS	URI do repositório do Amazon ECR
Europa (Paris)	`665651866788.dkr.ecr.eu-west-3.amazonaws.com/aws-guardduty-agent-ecs-ec2`
Europa (Frankfurt)	`323658145986.dkr.ecr.eu-central-1.amazonaws.com/aws-guardduty-agent-ecs-ec2`
Europa (Zurique)	`529164026651.dkr.ecr.eu-central-2.amazonaws.com/aws-guardduty-agent-ecs-ec2`
Europa (Estocolmo)	`591436053604.dkr.ecr.eu-north-1.amazonaws.com/aws-guarduty-agent-ecs-ec2`
Europa (Milão)	`266869475730.dkr.ecr.eu-south-1.amazonaws.com/aws-guarduty-agent-ecs-ec2`
Europa (Espanha)	`919611009337.dkr.ecr.eu-south-2.amazonaws.com/aws-guarduty-agent-ecs-ec2`
Ásia-Pacífico (Tóquio)	`533107202818.dkr.ecr.ap-northeast-1.amazonaws.com/aws-guardduty-agent-ecs-ec2`
Ásia-Pacífico (Seul)	`914738172881.dkr.ecr.ap-northeast-2.amazonaws.com/aws-guardduty-agent-ecs-ec2`
Asia Pacific (Osaka)	`273192626886.dkr.ecr.ap-northeast-3.amazonaws.com/aws-guardduty-agent-ecs-ec2`

Região da AWS	URI do repositório do Amazon ECR
Ásia-Pacífico (Singapura)	174946120834.dkr.ecr.ap-southeast-1.amazonaws.com/aws-guardduty-agent-ecs-ec2
Ásia-Pacífico (Sydney)	005257825471.dkr.ecr.ap-southeast-2.amazonaws.com/aws-guardduty-agent-ecs-ec2
Ásia-Pacífico (Jacarta)	510637619217.dkr.ecr.ap-southeast-3.amazonaws.com/aws-guardduty-agent-ecs-ec2
Ásia-Pacífico (Melbourne)	251357961535.dkr.ecr.ap-southeast-4.amazonaws.com/aws-guardduty-agent-ecs-ec2
Ásia-Pacífico (Mumbai)	251508486986.dkr.ecr.ap-south-1.amazonaws.com/aws-guarduty-agent-ecs-ec2
Ásia-Pacífico (Hyderabad)	950823858135.dkr.ecr.ap-south-2.amazonaws.com/aws-guarduty-agent-ecs-ec2
Ásia-Pacífico (Hong Kong)	258348409381.dkr.ecr.ap-east-1.amazonaws.com/aws-guardduty-agent-ecs-ec2
Canadá (Central)	354763396469.dkr.ecr.ca-central-1.amazonaws.com/aws-guardduty-agent-ecs-ec2
Oeste do Canadá (Calgary)	339712888787.dkr.ecr.ca-west-1.amazonaws.com/aws-guardduty-agent-ecs-ec2

Região da AWS	URI do repositório do Amazon ECR
América do Sul (São Paulo)	`758426053663.dkr.ecr.sa-east-1.amazonaws.com/aws-guardduty-agent-ecs-ec2`
Oriente Médio (Bahrein)	`536382113932.dkr.ecr.me-south-1.amazonaws.com/aws-guardduty-agent-ecs-ec2`
Oriente Médio (Emirados Árabes Unidos)	`000014521398.dkr.ecr.me-central-1.amazonaws.com/aws-guardduty-agent-ecs-ec2`
África (Cidade do Cabo)	`197869348890.dkr.ecr.af-south-1.amazonaws.com/aws-guardduty-agent-ecs-ec2`
Israel (Tel Aviv)	`870907303882.dkr.ecr.il-central-1.amazonaws.com/aws-guardduty-agent-ecs-ec2`
Ásia-Pacífico (Malásia)	`156041399949.dkr.ecr.ap-southeast-5.amazonaws.com/aws-guardduty-agent-ecs-ec2`
Ásia-Pacífico (Tailândia)	`054037130133.dkr.ecr.ap-southeast-7.amazonaws.com/aws-guardduty-agent-ecs-ec2`
México (Centro)	`311141559934.dkr.ecr.mx-central-1.amazonaws.com/aws-guardduty-agent-ecs-ec2`
Ásia-Pacífico (Taipei)	`259886477082.dkr.ecr.ap-east-2.amazonaws.com/aws-guardduty-agent-ecs-ec2`

Dois agentes de segurança no mesmo host subjacente

As instâncias do Amazon EC2 podem suportar vários tipos de workloads. Ao configurar o agente de segurança automatizado em uma instância do Amazon EC2, a mesma instância do EC2 pode ter outro agente de segurança por meio do EKS.

Visão geral do

Considere um cenário em que se tenha ativado o Monitoramento de runtime. Agora, você habilita o agente automatizado para o Amazon EKS por meio de GuardDuty. O agente automatizado para o Amazon EC2 também foi habilitado. Pode acontecer de o mesmo host subjacente ser instalado com dois agentes de segurança: um para o Amazon EKS e outro para o Amazon EC2. Isso pode resultar em dois agentes de segurança funcionando dentro do mesmo host, coletando eventos de tempo de execução e enviando-os para GuardDuty, e potencialmente gerando descobertas duplicadas.

Impacto

- Quando há mais de um agente de segurança em execução no mesmo host, sua conta pode ter o dobro das necessidades de processamento de CPU e memória. Para obter informações sobre os limites de CPU e memória para cada tipo de recurso, consulte Pré-requisitos para esse recurso.
- GuardDuty projetou o recurso Runtime Monitoring de forma que, mesmo que haja uma sobreposição de dois agentes de segurança coletando eventos de tempo de execução do mesmo host subjacente, sua conta será cobrada apenas por um fluxo de eventos de tempo de execução.

Como GuardDuty lida com vários agentes

GuardDuty detecta quando dois agentes de segurança estão sendo executados no mesmo host e designa somente um deles como o agente de segurança que coleta ativamente os eventos de tempo de execução. O segundo agente consumirá recursos mínimos do sistema para evitar qualquer impacto no desempenho de seus aplicativos.

GuardDuty considera os seguintes cenários:

- Quando uma instância do EC2 se enquadra no escopo dos agentes de segurança do Amazon EKS e do Amazon EC2, o agente de segurança EKS tem prioridade. Isso se aplicará somente quando o agente de segurança v1.1.0 ou superior for usado para o Amazon EC2. As versões mais antigas do agente continuarão sendo executadas e coletando eventos de runtime porque as versões mais antigas do agente não são afetadas pela priorização.

- Quando o Amazon EKS e o Amazon EC2 tiverem agentes de segurança GuardDuty gerenciados e sua instância do Amazon EC2 também for gerenciada por SSM, os dois agentes de segurança serão instalados no nível do host. Depois que os agentes estiverem instalados, GuardDuty decide qual agente de segurança continuará em execução. Quando os dois agentes de segurança estiverem em execução, em algum momento, apenas um deles coletará eventos de runtime.
- Quando os agentes de segurança associados ao EC2 e ao EKS são executados ao mesmo tempo, GuardDuty podem gerar descobertas duplicadas somente durante o período de sobreposição.

  Isso pode acontecer se:

  - Os agentes de segurança do EC2 e do EKS são configurados por meio de GuardDuty (automaticamente) ou
  - O recurso do Amazon EKS utilizado tem um agente de segurança automatizado.
- Quando o agente de segurança EKS já estiver em execução, se você implantar o agente de segurança EC2 manualmente no mesmo host subjacente e atender a todos os pré-requisitos, GuardDuty talvez não instale um segundo agente de segurança.

Monitoramento de execução do EKS em GuardDuty

O EKS Runtime Monitoring fornece cobertura de detecção de ameaças em tempo de execução para nós e contêineres do Amazon Elastic Kubernetes Service (Amazon EKS) em seu ambiente. AWS O EKS Runtime Monitoring usa um agente de GuardDuty segurança que adiciona visibilidade de tempo de execução às cargas de trabalho individuais do EKS, por exemplo, acesso a arquivos, execução de processos e conexões de rede. O agente GuardDuty de segurança ajuda a GuardDuty identificar contêineres específicos em seus clusters EKS que estão potencialmente comprometidos. Ele também pode detectar tentativas de escalar privilégios de um contêiner individual para o host EC2 subjacente e para o ambiente mais amplo. AWS

Com a disponibilidade do Runtime Monitoring, GuardDuty consolidou a experiência do console do EKS Runtime Monitoring em Runtime Monitoring. GuardDuty não migrará automaticamente suas configurações do EKS Runtime Monitoring em seu nome. Isso exige que você tome uma ação. Se quiser continuar usando somente o EKS Runtime Monitoring, você pode usar as APIs ou AWS CLI verificar e atualizar o status de configuração existente do EKS Runtime Monitoring. No entanto, GuardDuty recomenda Migração do Monitoramento de runtime do EKS para o Monitoramento de runtime e use o Runtime Monitoring para monitorar seus clusters do Amazon EKS.

Tópicos

- Configuração do Monitoramento de runtime do EKS para ambientes com várias contas (API)
- Configuração do Monitoramento de runtime do EKS para uma conta autônoma (API)
- Migração do Monitoramento de runtime do EKS para o Monitoramento de runtime

Configuração do Monitoramento de runtime do EKS para ambientes com várias contas (API)

Em ambientes com várias contas, somente a conta de GuardDuty administrador delegado pode ativar ou desativar o EKS Runtime Monitoring para as contas dos membros e gerenciar o gerenciamento de GuardDuty agentes para os clusters EKS pertencentes às contas dos membros em sua organização. As contas GuardDuty dos membros não podem modificar essa configuração em suas contas. A conta de GuardDuty administrador delegado gerencia suas contas de membros usando AWS Organizations. Para obter mais informações sobre ambientes com várias contas, consulte Gerenciar de várias contas.

Configurando o EKS Runtime Monitoring para uma conta de administrador delegado GuardDuty

Esta seção fornece etapas para configurar o EKS Runtime Monitoring e gerenciar o agente de GuardDuty segurança para os clusters EKS que pertencem à conta de GuardDuty administrador delegado.

Com base nas abordagens emImplantação do agente de segurança no Amazon EKS, você pode escolher uma abordagem preferida e seguir as etapas mencionadas na tabela a seguir.

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
Gerencie o agente de segurança por meio de GuardDuty (monitore todos os clusters EKS)	Execute a API updateDetector usando seu próprio ID de detector regional e transmitindo o nome de objeto `features` como `EKS_RUNTIME_MONITORING` e o status como `ENABLED`. Defina o status de `EKS_ADDON_MANAGEMENT` como `ENABLED`.

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
	GuardDuty gerenciará a implantação e as atualizações do agente de segurança para todos os clusters do Amazon EKS em sua conta. Como alternativa, você pode usar o AWS CLI comando usando seu próprio ID de detector regional. Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no https://console.aws.amazon.com/guardduty/console ou execute a ListDetectorsAPI. O exemplo a seguir habilita `EKS_RUNTIME_MONITORING` e `EKS_ADDON_MANAGEMENT` : `aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : "ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : "ENABLED"}] }]'`

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
Monitorar todos os clusters do EKS, mas excluir alguns deles (usando a tag de exclusão)	1. Adicione uma tag ao cluster do EKS que você deseja excluir do monitoramento. O par de chave-valor é `GuardDutyManaged -false`. Para obter mais informações sobre como adicionar a tag Como trabalhar com tags usando a CLI, a API ou o eksctl no Guia do usuário do Amazon EKS. 2. Para evitar a modificação de tags, exceto pelas entidades confiáveis, use a política fornecida em Impedir que as tags sejam modificadas, exceto por diretores autorizados no Guia do usuário do AWS Organizations . Nessa política, substitua estes detalhes: • Substitua *ec2:CreateTags* por `eks:TagResource` . • Substitua *ec2:DeleteTags* por `eks:UntagResource` . • Substituir *access-project* por `GuardDutyManaged` • *123456789012* Substitua pelo Conta da AWS ID da entidade confiável. Quando você tiver mais de uma entidade confiável , use o exemplo a seguir para adicionar vários `PrincipalArn` : `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]`

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
	3.

> **Note**
>
> Sempre adicione a tag de exclusão ao seu cluster EKS antes `STATUS` de `EKS_RUNTIME_MONITORING` definir of como`ENABLED`; caso contrário, o agente de GuardDuty segurança será implantado em todos os clusters EKS em sua conta.

Execute a API updateDetector usando seu próprio ID de detector regional e transmitindo o nome de objeto `features` como `EKS_RUNTIME_MONITORING` e o status como `ENABLED`.

Defina o status de `EKS_ADDON_MANAGEMENT` como `ENABLED`.

GuardDuty gerenciará a implantação e as atualizações do agente de segurança para todos os clusters do Amazon EKS que não foram excluídos do monitoramento.

Como alternativa, você pode usar o AWS CLI comando usando seu próprio ID de detector regional. Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no https://console.aws.amazon.com/guardduty/console ou execute a ListDetectorsAPI.

O exemplo a seguir habilita `EKS_RUNTIME_MONITORING` e `EKS_ADDON_MANAGEMENT` :

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
	`aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " ENABLED"}] }]'`

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
Monitorar clusters do EKS seletivos (usando a tag de inclusão)	1. Adicione uma tag ao cluster EKS que você deseja incluir no monitoramento. O par de chave-valor é `GuardDutyManaged -true`. Para obter mais informações sobre como adicionar a tag Como trabalhar com tags usando a CLI, a API ou o eksctl no Guia do usuário do Amazon EKS. 2. Para evitar a modificação de tags, exceto pelas entidades confiáveis, use a política fornecida em Impedir que as tags sejam modificadas, exceto por diretores autorizados no Guia do usuário do AWS Organizations . Nessa política, substitua estes detalhes: • Substitua *ec2:CreateTags* por `eks:TagResource` . • Substitua *ec2:DeleteTags* por `eks:UntagResource` . • Substituir *access-project* por `GuardDutyManaged` • *123456789012* Substitua pelo Conta da AWS ID da entidade confiável. Quando você tiver mais de uma entidade confiável , use o exemplo a seguir para adicionar vários `PrincipalArn` : `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 3. Execute a API updateDetector usando seu próprio ID de detector regional e transmitindo o nome de objeto

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
	`features` como `EKS_RUNTIME_MONITORING` e o status como `ENABLED`. Defina o status de `EKS_ADDON_MANAGEMENT` como `DISABLED`. GuardDuty gerenciará a implantação e as atualizações do agente de segurança para todos os clusters do Amazon EKS que foram marcados com o `true` par `GuardDutyManaged` -. Como alternativa, você pode usar o AWS CLI comando usando seu próprio ID de detector regional. Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no https://console.aws.amazon.com/guardduty/console ou execute a ListDetectorsAPI. O exemplo a seguir habilita `EKS_RUNTIME_MONITORING` e desabilita `EKS_ADDON_MANAGEMENT` : `aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " DISABLED"}] }]'`

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
Gerenciar o agente de segurança manualmente	1. Execute a API updateDetector usando seu próprio ID de detector regional e transmitindo o nome de objeto `features` como `EKS_RUNTIME_MONITORING` e o status como `ENABLED`. Defina o status de `EKS_ADDON_MANAGEMENT` como `DISABLED`. Como alternativa, você pode usar o AWS CLI comando usando seu próprio ID de detector regional. Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no https://console.aws.amazon.com/guardduty/console ou execute a ListDetectorsAPI. O exemplo a seguir habilita `EKS_RUNTIME_MONITORING` e desabilita `EKS_ADDON_MANAGEMENT` : `aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " DISABLED"}] }]'` 2. Para gerenciar o agente de segurança, consulte Como gerenciar o agente de segurança manualmente para o cluster Amazon EKS.

Auto-enable Monitoramento do EKS Runtime para todas as contas dos membros

Esta seção inclui etapas para habilitar o Monitoramento de runtime do EKS e gerenciar o agente de segurança para todas as contas de membros. Isso inclui a conta de GuardDuty administrador delegado, as contas de membros existentes e as novas contas que ingressam na organização.

Com base nas abordagens emImplantação do agente de segurança no Amazon EKS, você pode escolher uma abordagem preferida e seguir as etapas mencionadas na tabela a seguir.

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
Gerencie o agente de segurança por meio de GuardDuty (monitore todos os clusters EKS)	Para ativar seletivamente o EKS Runtime Monitoring para suas contas de membros, execute a operação da updateMemberDetectorsAPI usando a sua própria*detector ID*. Defina o status de `EKS_ADDON_MANAGEMENT` como `ENABLED`. GuardDuty gerenciará a implantação e as atualizações do agente de segurança para todos os clusters do Amazon EKS em sua conta. Como alternativa, você pode usar o AWS CLI comando usando seu próprio ID de detector regional. Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no https://console.aws.amazon.com/guardduty/console ou execute a ListDetectorsAPI. O exemplo a seguir habilita `EKS_RUNTIME_MONITORING` e `EKS_ADDON_MANAGEMENT` : `aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : "ENABLED"}] }]'` **Note** Você também pode passar uma lista de IDs de contas separadas por um espaço.

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
	Quando o código é executado com êxito, ele retorna uma lista vazia de `UnprocessedAccounts` . Se houver algum problema na alteração das configurações do detector de uma conta, esse ID de conta será listado junto com um resumo do problema.

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
Monitorar todos os clusters do EKS, mas excluir alguns deles (usando a tag de exclusão)	1. Adicione uma tag ao cluster do EKS que você deseja excluir do monitoramento. O par de chave-valor é `GuardDuty Managed -false`. Para obter mais informações sobre como adicionar a tag Como trabalhar com tags usando a CLI, a API ou o eksctl no Guia do usuário do Amazon EKS. 2. Para evitar a modificação de tags, exceto pelas entidades confiáveis, use a política fornecida em Impedir que as tags sejam modificadas, exceto por diretores autorizados no Guia do usuário do AWS Organizations . Nessa política, substitua estes detalhes: • Substitua *ec2:CreateTags* por `eks:TagResource` . • Substitua *ec2:DeleteTags* por `eks:UntagResource` . • Substituir *access-project* por `GuardDutyManaged` • *123456789012* Substitua pelo Conta da AWS ID da entidade confiável. Quando você tiver mais de uma entidade confiável, use o exemplo a seguir para adicionar vários `PrincipalArn` : `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 3. **Note** Sempre adicione a tag de exclusão ao seu cluster EKS antes `STATUS` de `EKS_RUNTIME_MONITORING` definir of como`ENABLED`; caso contrário, o agente de GuardDuty segurança será implantado em todos os clusters EKS em sua conta.

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
	Execute a API updateDetector usando seu próprio ID de detector regional e transmitindo o nome de objeto `features` como `EKS_RUNTIME_MONITORING` e o status como `ENABLED`. Defina o status de `EKS_ADDON_MANAGEMENT` como `ENABLED`. GuardDuty gerenciará a implantação e as atualizações do agente de segurança para todos os clusters do Amazon EKS que não foram excluídos do monitoramento. Como alternativa, você pode usar o AWS CLI comando usando seu próprio ID de detector regional. Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no https://console.aws.amazon.com/guardduty/console ou execute a ListDetectorsAPI. O exemplo a seguir habilita `EKS_RUNTIME_MONITORING` e `EKS_ADDON_MANAGEMENT` : `aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " ENABLED"}] }]'` **Note** Você também pode passar uma lista de IDs de contas separadas por um espaço.

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
	Quando o código é executado com êxito, ele retorna uma lista vazia de `UnprocessedAccounts`. Se houver algum problema na alteração das configurações do detector de uma conta, esse ID de conta será listado junto com um resumo do problema.

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
Monitorar clusters do EKS seletivos (usando a tag de inclusão)	1. Adicione uma tag ao cluster EKS que você deseja incluir no monitoramento. O par de chave-valor é `GuardDuty Managed -true`. Para obter mais informações sobre como adicionar a tag Como trabalhar com tags usando a CLI, a API ou o eksctl no Guia do usuário do Amazon EKS. 2. Para evitar a modificação de tags, exceto pelas entidades confiáveis, use a política fornecida em Impedir que as tags sejam modificadas, exceto por diretores autorizados no Guia do usuário do AWS Organizations . Nessa política, substitua estes detalhes: • Substitua *ec2:CreateTags* por `eks:TagResource` . • Substitua *ec2:DeleteTags* por `eks:UntagResource` . • Substituir *access-project* por `GuardDutyManaged` • *123456789012* Substitua pelo Conta da AWS ID da entidade confiável. Quando você tiver mais de uma entidade confiável, use o exemplo a seguir para adicionar vários `PrincipalArn` : `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 3. Execute a API updateDetector usando seu próprio ID de detector regional e transmitindo o nome de objeto `features` como `EKS_RUNTIME_MONITORING` e o status como `ENABLED`. Defina o status de `EKS_ADDON_MANAGEMENT` como `DISABLED`.

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
	GuardDuty gerenciará a implantação e as atualizações do agente de segurança para todos os clusters do Amazon EKS que foram marcados com o `true` par `GuardDutyManaged` -. Como alternativa, você pode usar o AWS CLI comando usando seu próprio ID de detector regional. Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no https://console.aws.amazon.com/guardduty/console ou execute a ListDetectorsAPI. O exemplo a seguir habilita `EKS_RUNTIME_MONITORING` e desabilita `EKS_ADDON_MANAGEMENT` : `aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " DISABLED"}] }]'` **Note** Você também pode passar uma lista de IDs de contas separadas por um espaço. Quando o código é executado com êxito, ele retorna uma lista vazia de `UnprocessedAccounts` . Se houver algum problema na alteração das configurações do detector de uma conta, esse ID de conta será listado junto com um resumo do problema.

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
Gerenciar o agente de segurança manualmente	1. Execute a API updateDetector usando seu próprio ID de detector regional e transmitindo o nome de objeto `features` como `EKS_RUNTIME_MONITORING` e o status como `ENABLED`. Defina o status de `EKS_ADDON_MANAGEMENT` como `DISABLED`. Como alternativa, você pode usar o AWS CLI comando usando seu próprio ID de detector regional. Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no https://console.aws.amazon.com/guardduty/console ou execute a ListDetectorsAPI. O exemplo a seguir habilita `EKS_RUNTIME_MONITORING` e desabilita `EKS_ADDON_MANAGEMENT` : `aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 555555555555 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " DISABLED"}] } ]'` 2. Para gerenciar o agente de segurança, consulte Como gerenciar o agente de segurança manualmente para o cluster Amazon EKS.

Configuração do Monitoramento de runtime do EKS para todas as contas-membro ativas existentes

Esta seção inclui as etapas para ativar o EKS Runtime Monitoring e gerenciar o agente de GuardDuty segurança para contas de membros ativos existentes em sua organização.

Com base nas abordagens emImplantação do agente de segurança no Amazon EKS, você pode escolher uma abordagem preferida e seguir as etapas mencionadas na tabela a seguir.

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
Gerencie o agente de segurança por meio de GuardDuty (monitore todos os clusters EKS)	Para ativar seletivamente o EKS Runtime Monitoring para suas contas de membros, execute a operação da updateMemberDetectorsAPI usando a sua própria*detector ID*. Defina o status de `EKS_ADDON_MANAGEMENT` como `ENABLED`. GuardDuty gerenciará a implantação e as atualizações do agente de segurança para todos os clusters do Amazon EKS em sua conta. Como alternativa, você pode usar o AWS CLI comando usando seu próprio ID de detector regional. Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no https://console.aws.amazon.com/guardduty/console ou execute a ListDetectorsAPI. O exemplo a seguir habilita `EKS_RUNTIME_MONITORING` e `EKS_ADDON_MANAGEMENT` : `aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : "ENABLED"}] }]'` **Note** Você também pode passar uma lista de IDs de contas separadas por um espaço. Quando o código é executado com êxito, ele retorna uma lista vazia de `UnprocessedAccounts` . Se houver algum problema na

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
	alteração das configurações do detector de uma conta, esse ID de conta será listado junto com um resumo do problema.

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
Monitorar todos os clusters do EKS, mas excluir alguns deles (usando a tag de exclusão)	1. Adicione uma tag ao cluster do EKS que você deseja excluir do monitoramento. O par de chave-valor é `GuardDuty Managed -false`. Para obter mais informações sobre como adicionar a tag Como trabalhar com tags usando a CLI, a API ou o eksctl no Guia do usuário do Amazon EKS. 2. Para evitar a modificação de tags, exceto pelas entidades confiáveis, use a política fornecida em Impedir que as tags sejam modificadas, exceto por diretores autorizados no Guia do usuário do AWS Organizations . Nessa política, substitua estes detalhes: • Substitua *`ec2:CreateTags`* por `eks:TagResource` . • Substitua *`ec2:DeleteTags`* por `eks:UntagResource` . • Substituir *`access-project`* por `GuardDutyManaged` • *`123456789012`* Substitua pelo Conta da AWS ID da entidade confiável. Quando você tiver mais de uma entidade confiável, use o exemplo a seguir para adicionar vários `PrincipalArn` : `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 3. **Note** Sempre adicione a tag de exclusão ao seu cluster EKS antes `STATUS` de `EKS_RUNTIME_MONITORING` definir of como`ENABLED`; caso contrário, o agente de GuardDuty segurança será implantado em todos os clusters EKS em sua conta.

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
	Para ativar seletivamente o EKS Runtime Monitoring para suas contas de membros, execute a operação da updateMemberDetectorsAPI usando a sua própria*detector ID*. Defina o status de `EKS_ADDON_MANAGEMENT` como `ENABLED`. GuardDuty gerenciará a implantação e as atualizações do agente de segurança para todos os clusters do Amazon EKS que não foram excluídos do monitoramento. Como alternativa, você pode usar o AWS CLI comando usando seu próprio ID de detector regional. Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no https://console.aws.amazon.com/guardduty/console ou execute a ListDetectorsAPI. O exemplo a seguir habilita `EKS_RUNTIME_MONITORING` e `EKS_ADDON_MANAGEMENT` : `aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " ENABLED"}] }]'` **Note** Você também pode passar uma lista de IDs de contas separadas por um espaço.

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
	Quando o código é executado com êxito, ele retorna uma lista vazia de `UnprocessedAccounts`. Se houver algum problema na alteração das configurações do detector de uma conta, esse ID de conta será listado junto com um resumo do problema.

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
Monitorar clusters do EKS seletivos (usando a tag de inclusão)	1. Adicione uma tag ao cluster EKS que você deseja incluir no monitoramento. O par de chave-valor é `GuardDuty Managed -true`. Para obter mais informações sobre como adicionar a tag Como trabalhar com tags usando a CLI, a API ou o eksctl no Guia do usuário do Amazon EKS. 2. Para evitar a modificação de tags, exceto pelas entidades confiáveis, use a política fornecida em Impedir que as tags sejam modificadas, exceto por diretores autorizados no Guia do usuário do AWS Organizations . Nessa política, substitua estes detalhes: • Substitua *`ec2:CreateTags`* por `eks:TagResource` . • Substitua *`ec2:DeleteTags`* por `eks:UntagResource` . • Substituir *`access-project`* por `GuardDutyManaged` • *`123456789012`* Substitua pelo Conta da AWS ID da entidade confiável. Quando você tiver mais de uma entidade confiável, use o exemplo a seguir para adicionar vários `PrincipalArn` : `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 3. Para ativar seletivamente o EKS Runtime Monitoring para suas contas de membros, execute a operação da updateMemberDetectorsAPI usando a sua própria*`detector ID`*. Defina o status de `EKS_ADDON_MANAGEMENT` como `DISABLED`.

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
	GuardDuty gerenciará a implantação e as atualizações do agente de segurança para todos os clusters do Amazon EKS que foram marcados com o `true` par `GuardDutyManaged` -. Como alternativa, você pode usar o AWS CLI comando usando seu próprio ID de detector regional. Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no https://console.aws.amazon.com/guardduty/console ou execute a ListDetectorsAPI. O exemplo a seguir habilita `EKS_RUNTIME_MONITORING` e desabilita `EKS_ADDON_MANAGEMENT` : `aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " DISABLED"}] }]'` **Note** Você também pode passar uma lista de IDs de contas separadas por um espaço. Quando o código é executado com êxito, ele retorna uma lista vazia de `UnprocessedAccounts` . Se houver algum problema na alteração das configurações do detector de uma conta, esse ID de conta será listado junto com um resumo do problema.

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
Gerenciar o agente de segurança manualmente	1. Para ativar seletivamente o EKS Runtime Monitoring para suas contas de membros, execute a operação da updateMemberDetectorsAPI usando a sua própria*detector ID*. Defina o status de `EKS_ADDON_MANAGEMENT` como `DISABLED`. Como alternativa, você pode usar o AWS CLI comando usando seu próprio ID de detector regional. Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no https://console.aws.amazon.com/guardduty/console ou execute a ListDetectorsAPI. O exemplo a seguir habilita `EKS_RUNTIME_MONITORING` e desabilita `EKS_ADDON_MANAGEMENT` : `aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 555555555555 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " DISABLED"}] } ]'` 2. Para gerenciar o agente de segurança, consulte Como gerenciar o agente de segurança manualmente para o cluster Amazon EKS.

Auto-enable Monitoramento de tempo de execução do EKS para novos membros

A conta de GuardDuty administrador delegado pode ativar automaticamente o EKS Runtime Monitoring e escolher uma abordagem de como gerenciar o agente de GuardDuty segurança para novas contas que ingressam na sua organização.

Com base nas abordagens emImplantação do agente de segurança no Amazon EKS, você pode escolher uma abordagem preferida e seguir as etapas mencionadas na tabela a seguir.

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas

Gerencie o agente de segurança por meio de GuardDuty (monitore todos os clusters EKS)	Para ativar seletivamente o EKS Runtime Monitoring para suas novas contas, invoque a operação da UpdateOrganizationConfigurationAPI usando a sua própria. *detector ID*
	
	Defina o status de `EKS_ADDON_MANAGEMENT` como `ENABLED`.
	
	GuardDuty gerenciará a implantação e as atualizações do agente de segurança para todos os clusters do Amazon EKS em sua conta.
	
	Como alternativa, você pode usar o AWS CLI comando usando seu próprio ID de detector regional. Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no https://console.aws.amazon.com/guardduty/console ou execute a ListDetectorsAPI.
	
	O exemplo a seguir habilita `EKS_RUNTIME_MONITORING` e `EKS_ADDON_MANAGEMENT` para uma única conta. Também é possível passar uma lista de IDs de conta separados por um espaço.
	
	Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no https://console.aws.amazon.com/guardduty/console ou execute a ListDetectorsAPI.
	
	`aws guardduty update-organization-configuration --detector-id 12abc34d567e8fa901bc2d34e56789f0 --autoEnable --features '[{"Name" : "EKS_RUNTIME_MONITORING", "AutoEnable": "NEW", "Addition`
	
	`IME_MONITORING", "AutoEnable": "NEW", "Addition`

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
	alConfiguration" : [{"Name" : "EKS_ADDON_MANAGEM ENT", "AutoEnable": "NEW"}] }]' Quando o código é executado com êxito, ele retorna uma lista vazia de `UnprocessedAccounts` . Se houver algum problema na alteração das configurações do detector de uma conta, esse ID de conta será listado junto com um resumo do problema.

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
Monitorar todos os clusters do EKS, mas excluir alguns deles (usando a tag de exclusão)	1. Adicione uma tag ao cluster do EKS que você deseja excluir do monitoramento. O par de chave-valor é `GuardDutyManaged -false`. Para obter mais informações sobre como adicionar a tag Como trabalhar com tags usando a CLI, a API ou o eksctl no Guia do usuário do Amazon EKS. 2. Para evitar a modificação de tags, exceto pelas entidades confiáveis, use a política fornecida em Impedir que as tags sejam modificadas, exceto por diretores autorizados no Guia do usuário do AWS Organizations . Nessa política, substitua estes detalhes: • Substitua *ec2:CreateTags* por `eks:TagResource` . • Substitua *ec2:DeleteTags* por `eks:UntagResource` . • Substituir *access-project* por `GuardDutyManaged` • *123456789012* Substitua pelo Conta da AWS ID da entidade confiável. Quando você tiver mais de uma entidade confiável , use o exemplo a seguir para adicionar vários `PrincipalArn` : `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]`

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
	3. **Note** Sempre adicione a tag de exclusão ao seu cluster EKS antes `STATUS` de `EKS_RUNTIME_MONITORING` definir of como`ENABLED`; caso contrário, o agente de GuardDuty segurança será implantado em todos os clusters EKS em sua conta. Para ativar seletivamente o EKS Runtime Monitoring para suas novas contas, invoque a operação da UpdateOrganizationConfigurationAPI usando a sua própria. *`detector ID`* Defina o status de `EKS_ADDON_MANAGEMENT` como `ENABLED`. GuardDuty gerenciará a implantação e as atualizações do agente de segurança para todos os clusters do Amazon EKS que não foram excluídos do monitoramento. Como alternativa, você pode usar o AWS CLI comando usando seu próprio ID de detector regional. Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no https://console.aws.amazon.com/guardduty/console ou execute a ListDetectorsAPI. O exemplo a seguir habilita `EKS_RUNTIME_MONITORING` e `EKS_ADDON_MANAGEMENT` para uma única conta. Também é possível passar uma lista de IDs de conta separados por um espaço.

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
	Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no https://console.aws.amazon.com/guardduty/console ou execute a ListDetectorsAPI. `aws guardduty update-organization-configuration --detector-id 12abc34d567e8fa901bc2d34e56789f0 --autoEnable --features '[{"Name" : "EKS_RUNTIME_MONITORING", "AutoEnable": "NEW", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "AutoEnable": "NEW"}] }]'` Quando o código é executado com êxito, ele retorna uma lista vazia de `UnprocessedAccounts`. Se houver algum problema na alteração das configurações do detector de uma conta, esse ID de conta será listado junto com um resumo do problema.

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
Monitorar clusters do EKS seletivos (usando a tag de inclusão)	1. Adicione uma tag ao cluster EKS que você deseja incluir no monitoramento. O par de chave-valor é `GuardDutyManaged -true`. Para obter mais informações sobre como adicionar a tag Como trabalhar com tags usando a CLI, a API ou o eksctl no Guia do usuário do Amazon EKS. 2. Para evitar a modificação de tags, exceto pelas entidades confiáveis, use a política fornecida em Impedir que as tags sejam modificadas, exceto por diretores autorizados no Guia do usuário do AWS Organizations . Nessa política, substitua estes detalhes: • Substitua *ec2:CreateTags* por `eks:TagResource` . • Substitua *ec2:DeleteTags* por `eks:UntagResource` . • Substituir *access-project* por `GuardDutyManaged` • *123456789012* Substitua pelo Conta da AWS ID da entidade confiável. Quando você tiver mais de uma entidade confiável , use o exemplo a seguir para adicionar vários `PrincipalArn` : `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 3. Para ativar seletivamente o EKS Runtime Monitoring para suas novas contas, invoque a operação da

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
	UpdateOrganizationConfigurationAPI usando a sua própria. *detector ID* Defina o status de EKS_ADDON_MANAGEMENT como DISABLED. GuardDuty gerenciará a implantação e as atualizaç ões do agente de segurança para todos os clusters do Amazon EKS que foram marcados com o true par GuardDutyManaged -. Como alternativa, você pode usar o AWS CLI comando usando seu próprio ID de detector regional. Para encontrar a opção detectorId para sua conta e região atual, consulte a página de configurações no https://console.aws.amazon.com/guardduty/console ou execute a ListDetectorsAPI. O exemplo a seguir habilita EKS_RUNTIME_MONITO RING e desabilita EKS_ADDON_MANAGEMENT para uma única conta. Também é possível passar uma lista de IDs de conta separados por um espaço. Para encontrar a opção detectorId para sua conta e região atual, consulte a página de configurações no https://console.aws.amazon.com/guardduty/console ou execute a ListDetectorsAPI. `aws guardduty update-organization-configu ration --detector-id 12abc34d567e8fa901 bc2d34e56789f0 --autoEnable --feature s '[{"Name" : "EKS_RUNTIME_MONITORING", "AutoEnable": "NEW", "AdditionalConfigu ration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "AutoEnable": "NEW"}] }]'`

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
	Quando o código é executado com êxito, ele retorna uma lista vazia de `UnprocessedAccounts` . Se houver algum problema na alteração das configurações do detector de uma conta, esse ID de conta será listado junto com um resumo do problema.

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
Gerenciar o agente de segurança manualmente	1. Para ativar seletivamente o EKS Runtime Monitoring para suas novas contas, invoque a operação da UpdateOrganizationConfigurationAPI usando a sua própria. *detector ID* Defina o status de `EKS_ADDON_MANAGEMENT` como `DISABLED`. Como alternativa, você pode usar o AWS CLI comando usando seu próprio ID de detector regional. Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no https://console.aws.amazon.com/guardduty/console ou execute a ListDetectorsAPI. O exemplo a seguir habilita `EKS_RUNTIME_MONITORING` e desabilita `EKS_ADDON_MANAGEMENT` para uma única conta. Também é possível passar uma lista de IDs de conta separados por um espaço. Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no https://console.aws.amazon.com/guardduty/console ou execute a ListDetectorsAPI. `aws guardduty update-organization-configuration --detector-id 12abc34d567e8fa901bc2d34e56789f0 --autoEnable --features '[{"Name" : "EKS_RUNTIME_MONITORING", "AutoEnable": "NEW", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "AutoEnable": "NEW"}] }]'` Quando o código é executado com êxito, ele retorna uma lista vazia de `UnprocessedAccounts`. Se

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
	houver algum problema na alteração das configurações do detector de uma conta, esse ID de conta será listado junto com um resumo do problema. 2. Para gerenciar o agente de segurança, consulte Como gerenciar o agente de segurança manualmente para o cluster Amazon EKS.

Habilitar o Monitoramento de runtime do EKS para contas-membro individuais ativas

Esta seção inclui as etapas para configurar o Monitoramento de runtime do EKS e gerenciar o agente de segurança para contas individuais de membros ativos.

Com base nas abordagens emImplantação do agente de segurança no Amazon EKS, você pode escolher uma abordagem preferida e seguir as etapas mencionadas na tabela a seguir.

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
Gerencie o agente de segurança por meio de GuardDuty (monitore todos os clusters EKS)	Para ativar seletivamente o EKS Runtime Monitorin g para suas contas de membros, execute a operação da updateMemberDetectorsAPI usando a sua própria*detector ID*. Defina o status de `EKS_ADDON_MANAGEMENT` como `ENABLED`. GuardDuty gerenciará a implantação e as atualizações do agente de segurança para todos os clusters do Amazon EKS em sua conta. Como alternativa, você pode usar o AWS CLI comando usando seu próprio ID de detector regional. Para encontrar a opção `detectorId` para sua conta e região atual,

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
	consulte a página de configurações no https://console.aws.amazon.com/guardduty/console ou execute a ListDetectorsAPI. O exemplo a seguir habilita `EKS_RUNTIME_MONITORING` e `EKS_ADDON_MANAGEMENT` : `aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " ENABLED"}] }]'` **Note** Você também pode passar uma lista de IDs de contas separadas por um espaço. Quando o código é executado com êxito, ele retorna uma lista vazia de `UnprocessedAccounts` . Se houver algum problema na alteração das configurações do detector de uma conta, esse ID de conta será listado junto com um resumo do problema.

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
Monitorar todos os clusters do EKS, mas excluir alguns deles (usando a tag de exclusão)	1. Adicione uma tag ao cluster do EKS que você deseja excluir do monitoramento. O par de chave-valor é `GuardDutyManaged -false`. Para obter mais informações sobre como adicionar a tag Como trabalhar com tags usando a CLI, a API ou o eksctl no Guia do usuário do Amazon EKS. 2. Para evitar a modificação de tags, exceto pelas entidades confiáveis, use a política fornecida em Impedir que as tags sejam modificadas, exceto por diretores autorizados no Guia do usuário do AWS Organizations . Nessa política, substitua estes detalhes: • Substitua *ec2:CreateTags* por `eks:TagResource` . • Substitua *ec2:DeleteTags* por `eks:UntagResource` . • Substituir *access-project* por `GuardDutyManaged` • *123456789012* Substitua pelo Conta da AWS ID da entidade confiável. Quando você tiver mais de uma entidade confiável , use o exemplo a seguir para adicionar vários `PrincipalArn` : `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]`

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
	3.

> **Note**
>
> Sempre adicione a tag de exclusão ao seu cluster EKS antes `STATUS` de `EKS_RUNTIME_MONITORING` definir of como`ENABLED`; caso contrário, o agente de GuardDuty segurança será implantado em todos os clusters EKS em sua conta.

Para ativar seletivamente o EKS Runtime Monitoring para suas contas de membros, execute a operação da updateMemberDetectorsAPI usando a sua própria*`detector ID`*.

Defina o status de `EKS_ADDON_MANAGEMENT` como `ENABLED`.

GuardDuty gerenciará a implantação e as atualizações do agente de segurança para todos os clusters do Amazon EKS que não foram excluídos do monitoramento.

Como alternativa, você pode usar o AWS CLI comando usando seu próprio ID de detector regional. Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no https://console.aws.amazon.com/guardduty/console ou execute a ListDetectorsAPI.

O exemplo a seguir habilita `EKS_RUNTIME_MONITORING` e `EKS_ADDON_MANAGEMENT` :

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas

```
aws guardduty update-member-detectors --
detector-id  12abc34d567e8fa901bc2d34e56
789f0  --account-ids  111122223333  --feature
s '[{"Name" : "EKS_RUNTIME_MONITORING",
 "Status" : "ENABLED", "AdditionalConfigu
ration" : [{"Name" : "EKS_ADDON_MANAGEMENT",
 "Status" : "ENABLED"}] }]'
```

> **Note**
>
> Você também pode passar uma lista de IDs de contas separadas por um espaço.

Quando o código é executado com êxito, ele retorna uma lista vazia de `UnprocessedAccounts` . Se houver algum problema na alteração das configurações do detector de uma conta, esse ID de conta será listado junto com um resumo do problema.

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
Monitorar clusters do EKS seletivos (usando a tag de inclusão)	1. Adicione uma tag ao cluster EKS que você deseja incluir no monitoramento. O par de chave-valor é `GuardDutyManaged -true`. Para obter mais informações sobre como adicionar a tag Como trabalhar com tags usando a CLI, a API ou o eksctl no Guia do usuário do Amazon EKS. 2. Para evitar a modificação de tags, exceto pelas entidades confiáveis, use a política fornecida em Impedir que as tags sejam modificadas, exceto por diretores autorizados no Guia do usuário do AWS Organizations . Nessa política, substitua estes detalhes: • Substitua *ec2:CreateTags* por `eks:TagResource` . • Substitua *ec2:DeleteTags* por `eks:UntagResource` . • Substituir *access-project* por `GuardDutyManaged` • *123456789012* Substitua pelo Conta da AWS ID da entidade confiável. Quando você tiver mais de uma entidade confiável , use o exemplo a seguir para adicionar vários `PrincipalArn` : `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 3. Para ativar seletivamente o EKS Runtime Monitoring para suas contas de membros, execute a operação

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
	da updateMemberDetectorsAPI usando a sua própria*detector ID*. Defina o status de EKS_ADDON_MANAGEMENT como DISABLED. GuardDuty gerenciará a implantação e as atualizaç ões do agente de segurança para todos os clusters do Amazon EKS que foram marcados com o true par GuardDutyManaged -. Como alternativa, você pode usar o AWS CLI comando usando seu próprio ID de detector regional. Para encontrar a opção detectorId para sua conta e região atual, consulte a página de configurações no https://console.aws.amazon.com/guardduty/console ou execute a ListDetectorsAPI. O exemplo a seguir habilita EKS_RUNTIME_MONITO RING e desabilita EKS_ADDON_MANAGEMENT : `aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : "ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : "DISABLED"}] }]'` **Note** Você também pode passar uma lista de IDs de contas separadas por um espaço.

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
	Quando o código é executado com êxito, ele retorna uma lista vazia de `UnprocessedAccounts`. Se houver algum problema na alteração das configurações do detector de uma conta, esse ID de conta será listado junto com um resumo do problema.

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
Gerenciar o agente de segurança manualmente	1. Para ativar seletivamente o EKS Runtime Monitoring para suas contas de membros, execute a operação da updateMemberDetectorsAPI usando a sua própria*detector ID*. Defina o status de `EKS_ADDON_MANAGEMENT` como `DISABLED`. Como alternativa, você pode usar o AWS CLI comando usando seu próprio ID de detector regional. Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no https://console.aws.amazon.com/guardduty/console ou execute a ListDetectorsAPI. O exemplo a seguir habilita `EKS_RUNTIME_MONITORING` e desabilita `EKS_ADDON_MANAGEMENT` : `aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 555555555555 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : "ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : "DISABLED"}] } ]'` 2. Para gerenciar o agente de segurança, consulte Como gerenciar o agente de segurança manualmente para o cluster Amazon EKS.

Configuração do Monitoramento de runtime do EKS para uma conta autônoma (API)

Uma conta autônoma é responsável pela decisão de ativar ou desativar um plano de proteção Conta da AWS em uma conta específica Região da AWS.

Se sua conta estiver associada a uma conta de GuardDuty administrador por meio AWS Organizations ou pelo método de convite, esta seção não se aplica à sua conta. Para obter mais informações, consulte Configuração do Monitoramento de runtime do EKS para ambientes com várias contas (API).

Depois de ativar o Runtime Monitoring, certifique-se de instalar o agente GuardDuty de segurança por meio de configuração automatizada ou implantação manual. Como parte da conclusão de todas as etapas listadas no procedimento a seguir, certifique-se de instalar o agente de segurança.

Com base nas abordagens emImplantação do agente de segurança no Amazon EKS, você pode escolher uma abordagem preferida e seguir as etapas mencionadas na tabela a seguir.

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
Gerencie o agente de segurança por meio de GuardDuty (monitore todos os clusters EKS)	1. Execute a API updateDetector usando seu próprio ID de detector regional e transmitindo o nome de objeto `features` como `EKS_RUNTIME_MONITORING` e o status como `ENABLED`. Defina o status de `EKS_ADDON_MANAGEMENT` como `ENABLED`. GuardDuty gerenciará a implantação e as atualizaç ões do agente de segurança para todos os clusters do Amazon EKS em sua conta. 2. Como alternativa, você pode usar o AWS CLI comando usando seu próprio ID de detector regional. Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
	https://console.aws.amazon.com/guardduty/console ou execute a ListDetectorsAPI. O exemplo a seguir habilita `EKS_RUNTIME_MONITORING` e `EKS_ADDON_MANAGEMENT` : `aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " ENABLED"}] }]'`

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
Monitorar todos os clusters do EKS, mas excluir alguns deles (usando a tag de exclusão)	1. Adicione uma tag ao cluster do EKS que você deseja excluir do monitoramento. O par de chave-valor é `GuardDutyManaged -false`. Para obter mais informações sobre como adicionar a tag Como trabalhar com tags usando a CLI, a API ou o eksctl no Guia do usuário do Amazon EKS. 2. Para evitar a modificação de tags, exceto pelas entidades confiáveis, use a política fornecida em Impedir que as tags sejam modificadas, exceto por diretores autorizados no Guia do usuário do AWS Organizations . Nessa política, substitua estes detalhes: • Substitua *ec2:CreateTags* por `eks:TagResource` . • Substitua *ec2:DeleteTags* por `eks:UntagResource` . • Substituir *access-project* por `GuardDutyManaged` • *123456789012* Substitua pelo Conta da AWS ID da entidade confiável. Quando você tiver mais de uma entidade confiável , use o exemplo a seguir para adicionar vários `PrincipalArn` : `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]`

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
	3. **Note** Sempre adicione a tag de exclusão ao seu cluster EKS antes `STATUS` de `EKS_RUNTIME_MONITORING` definir of como`ENABLED`; caso contrário, o agente de GuardDuty segurança será implantado em todos os clusters EKS em sua conta. Execute a API updateDetector usando seu próprio ID de detector regional e transmitindo o nome de objeto `features` como `EKS_RUNTIME_MONITORING` e o status como `ENABLED`. Defina o status de `EKS_ADDON_MANAGEMENT` como `ENABLED`. GuardDuty gerenciará a implantação e as atualizaç ões do agente de segurança para todos os clusters do Amazon EKS que não foram excluídos do monitoram ento. Como alternativa, você pode usar o AWS CLI comando usando seu próprio ID de detector regional. Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no https://console.aws.amazon.com/guardduty/console ou execute a ListDetectorsAPI. O exemplo a seguir habilita `EKS_RUNTIME_MONITORING` e `EKS_ADDON_MANAGEMENT` :

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
	`aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " ENABLED"}] }]'`

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
Monitorar clusters do EKS seletivos (usando a tag de inclusão)	1. Adicione uma tag ao cluster EKS que você deseja incluir no monitoramento. O par de chave-valor é `GuardDutyManaged -true`. Para obter mais informações sobre como adicionar a tag Como trabalhar com tags usando a CLI, a API ou o eksctl no Guia do usuário do Amazon EKS. 2. Para evitar a modificação de tags, exceto pelas entidades confiáveis, use a política fornecida em Impedir que as tags sejam modificadas, exceto por diretores autorizados no Guia do usuário do AWS Organizations . Nessa política, substitua estes detalhes: • Substitua *ec2:CreateTags* por `eks:TagResource` . • Substitua *ec2:DeleteTags* por `eks:UntagResource` . • Substituir *access-project* por `GuardDutyManaged` • *123456789012* Substitua pelo Conta da AWS ID da entidade confiável. Quando você tiver mais de uma entidade confiável , use o exemplo a seguir para adicionar vários `PrincipalArn` : `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 3. Execute a API updateDetector usando seu próprio ID de detector regional e transmitindo o nome de objeto

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
	`features` como `EKS_RUNTIME_MONITORING` e o status como `ENABLED`. Defina o status de `EKS_ADDON_MANAGEMENT` como `DISABLED`. GuardDuty gerenciará a implantação e as atualizações do agente de segurança para todos os clusters do Amazon EKS que foram marcados com o `true` par `GuardDutyManaged` -. Como alternativa, você pode usar o AWS CLI comando usando seu próprio ID de detector regional. Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no https://console.aws.amazon.com/guardduty/console ou execute a ListDetectorsAPI. O exemplo a seguir habilita `EKS_RUNTIME_MONITORING` e desabilita `EKS_ADDON_MANAGEMENT` : `aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " DISABLED"}] }]'`

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
Gerenciar o agente de segurança manualmente	1. Execute a API updateDetector usando seu próprio ID de detector regional e transmitindo o nome de objeto `features` como `EKS_RUNTIME_MONITORING` e o status como `ENABLED`. Defina o status de `EKS_ADDON_MANAGEMENT` como `DISABLED`. Como alternativa, você pode usar o AWS CLI comando usando seu próprio ID de detector regional. Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no https://console.aws.amazon.com/guardduty/console ou execute a ListDetectorsAPI. O exemplo a seguir habilita `EKS_RUNTIME_MONITORING` e desabilita `EKS_ADDON_MANAGEMENT` : `aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " DISABLED"}] }]'` 2. Para gerenciar o agente de segurança, consulte Como gerenciar o agente de segurança manualmente para o cluster Amazon EKS.

Migração do Monitoramento de runtime do EKS para o Monitoramento de runtime

Com o lançamento do GuardDuty Runtime Monitoring, a cobertura de detecção de ameaças foi expandida para contêineres do Amazon ECS e instâncias do Amazon EC2. A experiência do

Monitoramento de runtime do EKS agora foi consolidada no Monitoramento de runtime. Você pode ativar o Runtime Monitoring e gerenciar agentes de GuardDuty segurança individuais para cada tipo de recurso (instância do Amazon EC2, cluster do Amazon ECS e cluster do Amazon EKS) para o qual você deseja monitorar o comportamento do tempo de execução.

GuardDuty consolidou a experiência de console do EKS Runtime Monitoring em Runtime Monitoring. GuardDuty recomenda Verificação do status da configuração do Monitoramento de runtime do EKS Migração do Monitoramento de runtime do EKS para o Monitoramento de runtime e.

Como parte da migração para o Monitoramento de runtime, certifique-se de que Desativar o monitoramento de runtime do EKS. Isso é importante porque, se você optar posteriormente por desativar o Monitoramento de runtime e não desativar o Monitoramento de runtime do EKS, continuará incorrendo nos custos de uso do Monitoramento de runtime do EKS.

Para migrar do Monitoramento de runtime do EKS para o Monitoramento de runtime

1. O GuardDuty console suporta o EKS Runtime Monitoring como parte do Runtime Monitoring.

   Você pode começar a usar o Monitoramento de runtime por meio de Verificação do status da configuração do Monitoramento de runtime do EKS de sua organização e contas.

   Certifique-se de não desativar o Monitoramento de runtime do EKS antes de ativar o Monitoramento de runtime. Se você desativar o Monitoramento de runtime do EKS, o gerenciamento de complementos do Amazon EKS também será desativado. Continue com as etapas a seguir na ordem indicada.
2. Certifique-se de que você conhece todos os Pré-requisitos para habilitar o Monitoramento de runtime.
3. Ative o Monitoramento de runtime replicando as mesmas configurações da organização para o Monitoramento de runtime que você tem para o Monitoramento de runtime do EKS. Para obter mais informações, consulte Como habilitar o monitoramento de runtime.
   - Se você tiver uma conta autônoma, será necessário habilitar o Monitoramento de runtime.

     Se seu agente GuardDuty de segurança já estiver implantado, as configurações correspondentes serão replicadas automaticamente e você não precisará defini-las novamente.
   - Se você tiver uma organização com configurações de ativação automática, certifique-se de replicar as mesmas configurações de ativação automática para o Monitoramento de Runtime.

- Se você tiver uma organização com configurações definidas individualmente para contas de membros ativos existentes, certifique-se de ativar o Runtime Monitoring e configurar o agente de GuardDuty segurança para esses membros individualmente.

4. Depois de garantir que as configurações do Runtime Monitoring e do agente de GuardDuty segurança estejam corretas, desative o EKS Runtime Monitoring usando a API ou o AWS CLI comando.
5. (Opcional) se você quiser limpar qualquer recurso associado ao agente GuardDuty de segurança, consulteDesativação, desinstalação e remoção de recursos no Monitoramento de runtime.

Caso queira continuar usando o Monitoramento de runtime do EKS sem habilitar o Monitoramento de runtime, consulte Monitoramento de execução do EKS em GuardDuty. Com base no seu caso de uso, escolha as etapas para configurar o Monitoramento de runtime EKS para uma conta independente ou para várias contas de membros.

Verificação do status da configuração do Monitoramento de runtime do EKS

Use as seguintes APIs ou AWS CLI comandos para verificar o status da configuração existente do EKS Runtime Monitoring.

Para verificar o status da configuração existente do Monitoramento de runtime do EKS em sua conta

- Execute GetDetectorpara verificar o status da configuração da sua própria conta.
- Como alternativa, você pode executar o seguinte comando usando AWS CLI:

```
aws guardduty get-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
region us-east-1
```

Certifique-se de substituir o ID do detector da sua região Conta da AWS e da atual. Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no https://console.aws.amazon.com/guardduty/console ou execute a ListDetectorsAPI.

Para verificar o status da configuração existente do EKS Runtime Monitoring para sua organização (somente como uma conta de GuardDuty administrador delegada)

- Execute DescribeOrganizationConfigurationpara verificar o status da configuração da sua organização.

Também é possível executar o seguinte comando usando AWS CLI:

```
aws guardduty describe-organization-configuration --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --region us-east-1
```

Certifique-se de substituir o ID do detector pelo ID do detector da sua conta de GuardDuty administrador delegado e a Região pela sua região atual. Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no https://console.aws.amazon.com/guardduty/console ou execute a ListDetectorsAPI.

Desativação do monitoramento de runtime do EKS após a migração para o monitoramento de runtime

Depois de garantir que as atuais configurações da sua conta ou organização tenham sido replicadas para o Monitoramento de runtime, é possível desativar o Monitoramento de runtime EKS.

Para desativar o Monitoramento de runtime do EKS

- Para desativar o Monitoramento de runtime do EKS na sua conta

  Execute a UpdateDetectorAPI com sua própria região*detector-id*.

  Como alternativa, você pode usar o AWS CLI comando a seguir. *12abc34d567e8fa901bc2d34e56789f0*Substitua por sua própria região*detector-id*.

  ```
  aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
  features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : "DISABLED"}]'
  ```

- Para desabilitar o Monitoramento de runtime do EKS de contas de membros em sua organização

  Execute a UpdateMemberDetectorsAPI com a região *detector-id* da conta de GuardDuty administrador delegado da organização.

  Como alternativa, você pode usar o AWS CLI comando a seguir. *12abc34d567e8fa901bc2d34e56789f0*Substitua pela regional *detector-id* da conta de GuardDuty administrador delegado da organização e *111122223333* pela Conta da AWS ID da conta membro para a qual você deseja desativar esse recurso.

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --account-ids 111122223333 --features '[{"Name" : "EKS_RUNTIME_MONITORING",
 "Status" : "DISABLED"}]'
```

- Para atualizar as configurações de ativação automática do Monitoramento de runtime do EKS para sua organização

  Execute a etapa a seguir somente se tiver configurado as configurações de ativação automática do Monitoramento de runtime do EKS para novas (`NEW`) ou todas (`ALL`) as contas de membros da organização. Caso já tenha configurado como`NONE`, pode-se ignorar esta etapa.

  > **Note**
  >
  > Definir a configuração de ativação automática do Monitoramento de runtime do EKS como `NONE` significa que o Monitoramento de runtime do EKS não será ativado automaticamente para nenhuma conta membro existente ou quando uma nova conta membro ingressar na sua organização.

  Execute a UpdateOrganizationConfigurationAPI com a região *`detector-id`* da conta de GuardDuty administrador delegado da organização.

  Como alternativa, você pode usar o AWS CLI comando a seguir. *`12abc34d567e8fa901bc2d34e56789f0`*Substitua pela regional *`detector-id`* da conta de GuardDuty administrador delegado da organização. Substitua *`EXISTING_VALUE`* o pela sua configuração atual para ativação automática GuardDuty.

  ```
  aws guardduty update-organization-configuration --detector-
  id 12abc34d567e8fa901bc2d34e56789f0 --auto-enable-organization-members EXISTING_VALUE
   --features '[{"Name" : "EKS_RUNTIME_MONITORING", "AutoEnable": "NONE"}]'
  ```

GuardDuty versões de lançamento do agente de segurança

GuardDuty lança uma versão atualizada do agente de tempos em tempos. Quando GuardDuty gerencia o agente automaticamente, foi GuardDuty projetado para atualizar o agente em seu nome. Ao gerenciar o agente manualmente, é sua responsabilidade atualizar a versão do agente para os

tipos de recursos utilizados — instâncias do Amazon EC2, clusters do Amazon ECS e clusters do Amazon EKS.

As seções a seguir fornecem as versões de lançamento do GuardDuty Security Agent e as notas de versão associadas para todos os tipos de recursos compatíveis.

Tópicos

- GuardDuty versões do agente de segurança para instâncias do Amazon EC2
- GuardDuty versões de agentes de segurança para Amazon ECS-EC2 Bottlerocket
- GuardDuty versões do agente de segurança para AWS Fargate (Somente Amazon ECS)
- GuardDuty versões do agente de segurança para recursos do Amazon EKS
- Recursos adicionais – próximas etapas

GuardDuty versões do agente de segurança para instâncias do Amazon EC2

A tabela a seguir mostra o histórico de versões do agente GuardDuty de segurança do Amazon EC2.

Versão do distribuidor SSM	Versão do agente	Notas de atualização	Data de disponibilidade
v1.17.1	v1.17.1	Foi adicionado suporte para o Kernel 7.2. Na inicialização, o agente detecta o tipo de GuardDuty conectividade e tenta se conectar ao endpoint guardduty-data-v2 via link-local. Atualizações gerais dos recursos de segurança.	9 de setembro de 2026

Versão do distribuidor SSM	Versão do agente	Notas de atualização	Data de disponibilidade
v1.16.0	v1.16.0	Foi adicionado suporte para o Kernel 6.19, 7.0, 7.1. Foi adicionado suporte para Ubuntu 26.04, Debian 13, RedHat 10.2, CentOS Stream 10, Rocky Linux 10.1, Fedora 43 e Fedora 44. Para obter uma lista de todas as distribuições de sistema operacional verificadas para recursos do Amazon EC2, consulte Validação dos requisitos de arquitetura. Atualizações gerais dos recursos de segurança.	17 de julho de 2026

Versão do distribuidor SSM	Versão do agente	Notas de atualização	Data de disponibilidade
v1.15.0	v1.15.0	Novos recursos do agente para oferecer suporte à coleta otimizada de eventos, permitindo uma implantação mais rápida do filtro e uma maior velocidade de detecção. Atualizações gerais dos recursos de segurança.	14 de maio de 2026
v1.9.2	v1.9.2	Foi adicionado suporte para o Kernel 6.15, 6.16, 6.17, 6.18. Foi adicionado suporte para Alma Linux 9, Alma Linux 10 e SUSE Linux Enterprise Server 16. Para obter uma lista de todas as distribuições de sistema operacional verificadas para recursos do Amazon EC2, consulte Validação dos requisitos de arquitetura.	24 de fevereiro de 2026

Versão do distribuidor SSM	Versão do agente	Notas de atualização	Data de disponibilidade
v1.9.1	v1.9.1	Ajuste geral de desempenho e atualizações de recursos de segurança.	10 de novembro de 2025
v1.9.0	v1.9.0	Ajustes e aprimoramentos gerais de desempenho.	23 de outubro de 2025
v1.8.0	v1.8.0	Ajustes e aprimoramentos gerais de desempenho.	12 de agosto de 2025
v1.7.2	v1.7.1	Suporte aprimorado para instalação de agentes locais para distribuições Linux baseadas em RPM.	23 de julho de 2025

Versão do distribuidor SSM	Versão do agente	Notas de atualização	Data de disponibilidade
v1.7.1	1.7.1	Foi adicionado suporte para o Fedora 40 e o Fedora 41. Para obter uma lista de todas as distribuições de sistema operacional verificadas para recursos do Amazon EC2, consulte Validação dos requisitos de arquitetura. Ajustes e aprimoramentos gerais de desempenho.	3 de junho de 2025

Versão do distribuidor SSM	Versão do agente	Notas de atualização	Data de disponibilidade
v1.7.0	v1.7.0	Foi adicionado suporte para Oracle Linux versões 8.9 e 9.3 e Rocky Linux versão 9.5. Para obter uma lista de todas as distribuições de sistema operacional verificadas para recursos do Amazon EC2, consulte Validação dos requisitos de arquitetura. Resolução aprimorada de ID de contêiner. Ajustes e aprimoramentos gerais de desempenho.	3 de abril de 2025
v1.6.0	v1.6.0	Ajustes e aprimoramentos gerais de desempenho.	6 de fevereiro de 2025

Versão do distribuidor SSM	Versão do agente	Notas de atualização	Data de disponibilidade
v1.5.0	v1.5.0	Foi adicionado suporte para CentOS Stream 9.0, RedHat 9.4, Fedora 34.0 e Ubuntu 24.04. Suporte para instâncias ARM para descobertas `.../MetadataDNSRebind` . Ajustes e aprimoramentos gerais de desempenho.	20 de novembro de 2024
v1.3.1	v1.3.1	Compatível com resolvedores de DNS personalizados.	12 de setembro de 2024
v1.3.0	v1.3.0	Ajustes e aprimoramentos gerais de desempenho. Inclui suporte para capturar sinais de segurança adicionais para o futuroGuardDuty Tipos de descoberta de monitoramento de tempo de execução.	19 de agosto de 2024

Versão do distribuidor SSM	Versão do agente	Notas de atualização	Data de disponibilidade
v1.2.0	v1.2.0	Suporte a distribuições de sistema operacional Ubuntu 20.04, Ubuntu 22.04, Debian 11 e Debian 12. Compatível com kernel 6.5 e 6.8. Ajustes e aprimoramentos gerais de desempenho.	13 de junho de 2024

Versão do distribuidor SSM	Versão do agente	Notas de atualização	Data de disponibilidade
v1.1.0	v1.1.0	Oferece suporte à configuração GuardDuty automatizada de agentes no Runtime Monitoring para instâncias do Amazon EC2. Compatível com novos sinais de segurança e descobertas divulgados com o anúncio da disponibilidade geral do Monitoramento de Runtime para instâncias do EC2. Ajustes e aprimoramentos gerais de desempenho.	26 de março de 2024
v1.0.2	v1.0.2	Compatível com as AMIs mais recentes do Amazon ECS.	2 de fevereiro de 2024

Versão do distribuidor SSM	Versão do agente	Notas de atualização	Data de disponibilidade
v1.0.1	v1.0.1	As versões do agente lançadas antes da v1.0.2 são incompatíveis com as AMIs do Amazon ECS lançadas após 31 de janeiro de 2024. Ajustes e aprimoramentos gerais de desempenho.	23 de janeiro de 2024
v1.0.0	v1.0.0	Versão inicial da instalação do RPM. As versões do agente lançadas antes da v1.0.2 são incompatíveis com as AMIs do Amazon ECS lançadas após 31 de janeiro de 2024.	26 de novembro de 2023

GuardDuty versões de agentes de segurança para Amazon ECS-EC2 Bottlerocket

A tabela a seguir mostra o histórico de versões do agente de GuardDuty segurança para instâncias do Amazon ECS-EC2 Bottlerocket. O agente é executado como um contêiner host no Bottlerocket e na versão ECS-2 `v1.62.1` otimizada da ECS-3 AMI ou superior.

Versão SSM Distributor	Versão do agente	Notas de atualização	Data de disponibilidade
v1.17.1	v1.17.1	Foi adicionado suporte para o Kernel 7.2. Na inicialização, o agente detecta o tipo de GuardDuty conectividade e tenta se conectar ao endpoint guardduty-data-v2 via link-local. Atualizações gerais dos recursos de segurança.	9 de setembro de 2026
v1.16.0	v1.16.0	Lançamento inicial do agente de GuardDuty segurança para instâncias do Amazon ECS-EC2 Bottlerocket. Suporta Bottlerocket ECS-2 e ECS-3 variantes (x86_64 e aarch64).	17 de julho de 2026

GuardDuty versões do agente de segurança para AWS Fargate (Somente Amazon ECS)

A tabela a seguir mostra o histórico de versões do agente de GuardDuty segurança do Fargate (somente Amazon ECS).

Versão do agente	Imagem do contêiner	Notas de atualização	Data de disponibilidade
v1.17.1	x86_64 (AMD64): `sha256:27b27c489113ae83a272b5c98112e043f66faf8379838bb38e2d815dd6dfbf3a` Graviton (ARM64): `sha256:195078e48505cb05b06e61df255fc85a6d7917b28678956c75b11e69855bdff3`	Foi adicionado suporte para o Kernel 7.2. Na inicialização, o agente detecta o tipo de GuardDuty conectividade e tenta se conectar ao endpoint guardduty-data-v2 via link-local. Atualizações gerais dos recursos de segurança.	09 de setembro de 2026
v1.16.0	x86_64 (AMD64): `sha256:711fa37e2cce0417ba3310d81439d6b11170e446f685146b36916e4e38c1560d` Graviton (ARM64): `sha256:6851e00893eee958085a`	Atualizações gerais dos recursos de segurança.	17 de julho de 2026

Versão do agente	Imagem do contêiner	Notas de atualização	Data de disponibilidade
	daccddf91 bdc009ebd dcd46b4da 6fb1962b1 32d47454		
v1.15.0	x86_64 (AMD64): sha256:66 446df341b ee1a1e218 aa46b7807 d0d047026 6c8f374c5 dbd97efcd b8356348 Graviton (ARM64): sha256:b0 def2aa8ca b6b2060c7 03f386fdb 29dc41660 54e0509a9 362b21a6e d7f9def7	Novos recursos do agente para oferecer suporte à coleta otimizada de eventos, permitindo uma implantação mais rápida do filtro e uma maior velocidade de detecção. Atualizações gerais dos recursos de segurança.	28 de maio de 2026

Versão do agente	Imagem do contêiner	Notas de atualização	Data de disponibilidade
v1.9.0	x86_64 (AMD64): `sha256:fd9acaa2326f180f0ed0c5a25d8ff0a2d0498a6e900c34c68d4e973ea7fb26a8` Graviton (ARM64): `sha256:0b04f8c28956684e752677bfd83dbc45afc8a43f7791fa44667b8078ba48a295`	Ajustes de desempenho gerais e aprimoramentos de segurança.	28 de outubro de 2025

Versão do agente	Imagem do contêiner	Notas de atualização	Data de disponibilidade
v1.8.0	x86_64 (AMD64): `sha256:4425417f39e38b24c1be428bacad1dad53e0645530dcf4422436353bfe358e3a` Graviton (ARM64): `sha256:aff069418fd6825846f8f575c49906a67c8a446d12d9ed0d21ab95bd0d05497b`	Ajustes e aprimoramentos gerais de desempenho.	12 de agosto de 2025

Versão do agente	Imagem do contêiner	Notas de atualização	Data de disponibilidade
v1.7.0	x86_64 (AMD64): `sha256:bf9197abdf853607e5fa392b4f97ccdd6ca56dd179be3ce8849e552d96582ac8` Graviton (ARM64): `sha256:56c8683c948bcd82c0dbcebf755204365ac7285994693c11717bd45f86e279c2`	Resolução aprimorada de ID de contêiner. Ajustes e aprimoramentos gerais de desempenho.	04 de abril de 2025

Versão do agente	Imagem do contêiner	Notas de atualização	Data de disponibilidade
v1.6.0	x86_64 (AMD64): `sha256:c8dea71d372bc47b2f236f7a091b9a9b06bc8193c1cfe4c9346eb50f89258897` Graviton (ARM64): `sha256:f4032a566b90537646c2a987bef42eca1b498078ccc58a848603f877971a8dbe`	Ajustes e aprimoramentos gerais de desempenho.	6 de fevereiro de 2025

Versão do agente	Imagem do contêiner	Notas de atualização	Data de disponibilidade
v1.5.0	x86_64 (AMD64): `sha256:5e6fdc41f9eb748219d0498cd6c1dba6a19d875daec50167a0ac80e5028eac54` Graviton (ARM64): `sha256:d56801ff6864d601474010 3b70b1c38431851358d182613bede20fe21090e734`	Suporte para tarefas ARM para descobertas `.../MetadataDNSRebind` . Ajustes e aprimoramentos gerais de desempenho.	14 de novembro de 2024

Versão do agente	Imagem do contêiner	Notas de atualização	Data de disponibilidade
v1.4.1	x86_64 (AMD64): `sha256:ef36a11151ec2d3d7db22273bfb954750dee76f0ac7bec37a7ba7e74c3de1c78` Graviton (ARM64): `sha256:a8844544a59d6b4cba98f8e528b513ac2d97432f208e3ad497cc16b331aa9faa`	Hardening das imagens do contêiner. Ajustes e aprimoramentos gerais de desempenho.	24 de outubro de 2024

Versão do agente	Imagem do contêiner	Notas de atualização	Data de disponibilidade
v1.3.1	x86_64 (AMD64): `sha256:a6e2307d796e2875907bc4c1c69622c906f3192ddc42ef27b99e0a8f0979f3e0` Graviton (ARM64): `sha256:ad1b6539d806edb504f17e6bcfb8b4026c5e822300afc31c0d23c6a08f9b99e9`	Compatível com resolvedores de DNS personalizados.	11 de setembro de 2024

Versão do agente	Imagem do contêiner	Notas de atualização	Data de disponibilidade

v1.3.0	x86_64 (AMD64):
	`sha256:f1ad3fb2dc55a1110c60eecf4453b9f9c02f29acb261df39814e7d29296bf831`
	
	Graviton (ARM64):
	`sha256:ff81a755d46681e409f55a95beedae9ebbcf5336e1c0b1e6348af7c6518bdbb1`
		Ajustes e aprimoramentos gerais de desempenho.
		
		Inclui suporte para capturar sinais de segurança adicionais para o futuro GuardDuty GuardDuty Tipos de descoberta de monitoramento de tempo de execução.
			9 de agosto de 2024

Versão do agente	Imagem do contêiner	Notas de atualização	Data de disponibilidade

v1.2.0	x86_64 (AMD64):
	`sha256:1dbad20ac2dc66d52d00bb28dde4281fe0d3c5f261b1649b247c2369d9e26b93`
	
	Graviton (ARM64):
	`sha256:91930f8446f5f95b93b8ccb18773992affa401eb3f42da89d68077a56bafa6cd`
		Ajustes e aprimoramentos gerais de desempenho.	31 de maio de 2024

Versão do agente	Imagem do contêiner	Notas de atualização	Data de disponibilidade
v1.1.0	x86_64 (AMD64): `sha256:83ce3cf2ef85a349ed1797a8cf30a008ac5d8c9f673f2835823957e9dcf71657` Graviton (ARM64): `sha256:0d4b61648d7bdeab8ab8d94684f805498927c7d437d318204dcccfe8c9383dc7`	É compatível com novos sinais e descobertas de segurança. Ajustes e aprimoramentos gerais de desempenho.	01 de maio de 2024

Versão do agente	Imagem do contêiner	Notas de atualização	Data de disponibilidade
v1.0.1	x86_64 (AMD64): `sha256:9f8cd438fb66f62d09bfc641286439f7ed5177988a314a6021ef4ff880642e68` Graviton (ARM64): `sha256:82c66bb615bd0d1e96db77b1f1fb51dc03220caa593b1962249571bf7147d1b7`	Ajustes e aprimoramentos gerais de desempenho.	26 de janeiro de 2024

Versão do agente	Imagem do contêiner	Notas de atualização	Data de disponibilidade
v1.0.0	x86_64 (AMD64): `sha256:359b8b014e5076c625daa1056090e522631587a7afa3b2e055edda6bd1141017` Graviton (ARM64): `sha256:b9438690fa8a86067180a11658bec0f4f838ae3fbd225d04b9306250648b3984`	Lançamento inicial do agente de GuardDuty segurança para AWS Fargate (somente Amazon ECS).	26 de novembro de 2023

GuardDuty versões do agente de segurança para recursos do Amazon EKS

GuardDuty lança uma versão atualizada do agente de tempos em tempos. Quando GuardDuty gerencia o agente automaticamente, ele é projetado para gerenciar as atualizações do agente em seu nome. Ao gerenciar o agente manualmente, você é responsável por atualizar a versão do agente para seus clusters do Amazon EKS.

Antes de atualizar o agente para uma versão específica, adicione o registro GuardDuty de imagens `allowed-container-registries` em seu controlador de admissão. Para obter mais informações, consulte Agente de hospedagem de repositórios Amazon ECR GuardDuty.

A tabela a seguir mostra o histórico de versões do GuardDuty agente complementar Amazon EKS.

Versão do agente	Imagem do contêiner	Notas de atualização	Data de disponibilidade	Término do suporte[1] padrão
v1.17.1	x86_64 (AMD64): `sha256:8d772f754e9af50a63ab6af74ea24c12a5a3fb8a803c7cbc35ffaca3746c0540` Graviton (ARM64): `sha256:e5531367e9ffa539e409e99bbf49e804f01fdd894ee9322858b9bca703cd4016`	Foi adicionado suporte para o Kernel 6.19, 7.0, 7.1. Na inicialização, o agente detecta o tipo de GuardDuty conectividade e tenta se conectar ao endpoint guardduty-data-v2 via link-local. Atualizações gerais dos recursos de segurança.	09 de setembro de 2026	–
v1.16.0	x86_64 (AMD64): `sha256:8a4ef4b5b5e6fce0a4b5a13922e65179293ee15a8812a2c7678b1c4b31e1f305`	Foi adicionado suporte para o Kernel 6.19, 7.0, 7.1. Atualizações gerais dos recursos de segurança.	17 de julho de 2026	–

Versão do agente	Imagem do contêiner	Notas de atualização	Data de disponibilidade	Término do suporte[1] padrão
	Graviton (ARM64): `sha256:0a73c1d905a39db94f6ea37d98784dac84961e9199935fae20345de7aa3a57b7`			
v1.15.0	x86_64 (AMD64): `sha256:512642a5f9d9a316aa9100368acfdbae2481be7a5cfe9929571c1bb6e19c66fe` Graviton (ARM64): `sha256:f017e755615ae999fe5f163886f681508e8f53feea7e64e7ada733cdedb368d8`	Novos recursos do agente para oferecer suporte à coleta otimizada de eventos, permitindo uma implantação mais rápida do filtro e uma maior velocidade de detecção. Atualizações gerais dos recursos de segurança.	14 de maio de 2026	–

Versão do agente	Imagem do contêiner	Notas de atualização	Data de disponibilidade	Término do suporte[1] padrão
v1.12.2	x86_64 (AMD64): `sha256:06c25ab9fff7ee93048e5f34148c9627366323 5937199b4bd2e28b5ee2e5c080` Graviton (ARM64): `sha256:f89962d971350ff6ab408cf6ec7bca9dd06152 f0172b7f9c68ae770cc0fc4598`	Atualizações gerais dos recursos de segurança.	26 de março de 2026	–

Versão do agente	Imagem do contêiner	Notas de atualização	Data de disponibilidade	Término do suporte[1] padrão
v1.12.1	x86_64 (AMD64): `sha256:f29a597745e5acff48809bebac7d8091bbc38229453dd26710c549b817362491` Graviton (ARM64): `sha256:089cebdc7e891177e107a099c9a4e362d9d74b5362cd374b448a16078040f6c6`	Ajuste geral de desempenho e atualizações de recursos de segurança.	17 de novembro de 2025	–

Versão do agente	Imagem do contêiner	Notas de atualização	Data de disponibilidade	Término do suporte[1] padrão
v1.11.0	x86_64 (AMD64): `sha256:7c398fd50dee5fe493c361aa7fe191e094ddfa000c65b449a9ed6a5cd53610e7` Graviton (ARM64): `sha256:98a547b47d4770f45e75eb9730c807d9265722ca2f391e0aa5cb19e487ab455f`	Foi adicionado o suporte para as distribuições de sistema operacional Fedora 40 e Fedora 41. Para obter mais informações, consulte Validação dos requisitos de arquitetura (para EKS). Ajustes de desempenho gerais e aprimoramentos de segurança.	29 de agosto de 2025	–

Versão do agente	Imagem do contêiner	Notas de atualização	Data de disponibilidade	Término do suporte[1] padrão
v1.10.0	x86_64 (AMD64): `sha256:6dcbe5b055e1ef0af903071ede0b08f755ad5b7e9774a67df5399efdaa1f3d7d` Graviton (ARM64): `sha256:f05368822689610a4bab543abf93d3e070b1b559e62a2e67d82dfa9837600f72`	Resolução aprimorada de ID de contêiner. Ajustes e aprimoram entos gerais de desempenho.	04 de abril de 2025	–

Versão do agente	Imagem do contêiner	Notas de atualização	Data de disponibilidade	Término do suporte[1] padrão
v1.9.0	x86_64 (AMD64): `sha256:51c5789ef6570f9bec879ac48a8f4769718cbc31e45430032569917e219af63f` Graviton (ARM64): `sha256:9c2f74e7ea0827b7e422ae4c91fffc6c2bc41a1cdb96c7191d05259d337154e1`	Ajustes e aprimoramentos gerais de desempenho.	02 de março de 2025	–

Versão do agente	Imagem do contêiner	Notas de atualização	Data de disponibilidade	Término do suporte[1] padrão
v1.8.1*	x86_64 (AMD64): `sha256:f2ce8cf89dbe17e3388cecb35053544dadf21af7770545f8d4b50384076aff47` Graviton (ARM64): `sha256:30f586e4b694e704bcafadfa9081ab0aeff3cfbcde39743a0f1e24f77d79627f`	Foi adicionado o suporte para CentOS Stream 9.0, RedHat 9.4, Fedora 34.0 e Ubuntu 24.04. Suporte para instâncias ARM para descoberta `.../MetadataDNSRebind` . Ajustes e aprimoramentos gerais de desempenho.	23 de novembro de 2024	–

Versão do agente	Imagem do contêiner	Notas de atualização	Data de disponibilidade	Término do suporte[1] padrão
v1.7.1	x86_64 (AMD64): `sha256:b8b86b5d0872c8b67fecf64ec3d17266636054 5435a1752447d510951a7fd749` Graviton (ARM64): `sha256:40ac4cfc354fd430ba7897ca1632e9a500ed13eeb0c315c5bcad38680e76b6e9`	Ajustes e aprimoram entos gerais de desempenho. Inclui suporte para capturar sinais de segurança adicionais para o futuroGuardDuty Tipos de descoberta de monitoramento de tempo de execução. Compatível com resolvedores de DNS personali zados.	13 de setembro de 2024	–

Versão do agente	Imagem do contêiner	Notas de atualização	Data de disponibilidade	Término do suporte[1] padrão
v1.7.0	x86_64 (AMD64): `sha256:f3a2a8806e6c2a7fd63a91cccf6f7dffcd7e68554a423d610cea8c7e8f2185ec` Graviton (ARM64): `sha256:b1a6db35a072c0de3c695e5e909a03e6c4e1fdbe47ecfaeb2784435cf67ebe0a`	Ajustes e aprimoramentos gerais de desempenho. Inclui suporte para capturar sinais de segurança adicionais para o futuroGuardDuty Tipos de descoberta de monitoramento de tempo de execução.	17 de agosto de 2024	–

Versão do agente	Imagem do contêiner	Notas de atualização	Data de disponibilidade	Término do suporte[1] padrão
v1.6.1	x86_64 (AMD64): `sha256:30650708a6601f6d6b9046f54b30f5fd65af296b1e40b8c24426b9bdb07c3ab1` Graviton (ARM64): `sha256:5f637c42ffb306b20f776d9d83e1e0b4be40ce245be44afcf43a8902b4d71019`	Ajustes e aprimoramentos gerais de desempenho.	14 de maio de 2024	–

Versão do agente	Imagem do contêiner	Notas de atualização	Data de disponibilidade	Término do suporte[1] padrão
v1.6.0	x86_64 (AMD64): `sha256:7dabcbee30d8b053676752fbc19e89f77272d9a6a53cc93731f5872180ef9010` Graviton (ARM64): `sha256:9710f53afccdf4f22b265a1a6fc27f1469403af1f7d5d08c4869a7269cdd2650`	• Oferece suporte à configuração GuardDuty automatizada de agentes para EKS/EC2 recursos. • É compatível com os novos sinais e descobertas de segurança. Para obter mais informações, consulte Tipos de eventos de tempo de execução coletados que GuardDuty usam e GuardDuty Tipos de descoberta de monitoramento de tempo de execução. • Ajustes e aprimoramentos gerais	29 de abril de 2024	–

Versão do agente	Imagem do contêiner	Notas de atualização	Data de disponibilidade	Término do suporte[1] padrão
		de desempenho.		
v1.5.0	x86_64 (AMD64): `sha256:e09a4e70af4058a212f172cc8eb3fc23ad9bed547ed609faa2bb82cf7cc5532d` Graviton (ARM64): `sha256:afc9a3f8f17ae12499d76069efcf1b46271a5a4b2b3f6ba5de54637b8f55d5c6`	• Ajustes e aprimoramentos gerais de desempenho. • Aprimoramentos de segurança, incluindo novos tipos de eventos em Tipos de eventos de runtime coletados. • Aprimoramentos de desempenho no uso da CPU.	07 de março de 2024	–

Versão do agente	Imagem do contêiner	Notas de atualização	Data de disponibilidade	Término do suporte[1] padrão
v1.4.1	x86_64 (AMD64): `sha256:66d49192776 3742660fa a87cc2c39 bb97b7873 039157ae8 b90bc999c b73d0b9c` Graviton (ARM64): `sha256:53 7a330b2dd 82357024f b6daeb876 1034b7def d43b10dff e0792c9e6 d0778b40`	Ajustes e aprimoram entos gerais de desempenho.	16 de janeiro de 2024	–

Versão do agente	Imagem do contêiner	Notas de atualização	Data de disponibilidade	Término do suporte[1] padrão
v1.4.0	x86_64 (AMD64): `sha256:848ce13d9430bad554ac23d4699551505326ada2a88e1a721fe9f86b56b52c0f` Graviton (ARM64): `sha256:0c650aeafeeb5f2bcb8b989ac849bedc1fae1a4de1cf6306ffdd9c6aebe67f8e`	O ponto de montagem do manifesto permite uma melhor coleta de dados AppArmor configuração no manifesto Coletar argumento da linha de comando Ajustes e aprimoram entos gerais de desempenho	21 de dezembro de 2023	–

Versão do agente	Imagem do contêiner	Notas de atualização	Data de disponibilidade	Término do suporte[1] padrão
v1.3.1	x86_64 (AMD64): `sha256:55578fcb7b73097ade5c8404390ef16cf76a7b568490abaae01ac75992b3ea29` Graviton (ARM64): `sha256:e3ce8d66ac2121f8d476eb58f8bc50ab51336647615eb7cf514c21421cb818fd`	Os patches e as atualizações de segurança importantes.	23 de outubro de 2023	–

Versão do agente	Imagem do contêiner	Notas de atualização	Data de disponibilidade	Término do suporte[1] padrão
v1.3.0	x86_64 (AMD64): `sha256:6dace2337dfbb7609811be89fb4b23ae0b865f1027ad78fbe69530bfbd46c694` Graviton (ARM64): `sha256:4928a7c6ef40e77c8ec95841323bb9a110db31f12c0ee7ab965e08b43efd01bb`	Compatível com a plataforma Ubuntu Compatível com o Kubernetes versão 1.28 Aprimoram entos gerais de performance e melhoria da estabilidade.	5 de outubro de 2023	–

Versão do agente	Imagem do contêiner	Notas de atualização	Data de disponibilidade	Término do suporte[1] padrão
v1.2.0	x86_64 (AMD64): `sha256:d610413d662ec042057f05d6942496d7f2c08e9f5a077ea307ffdb5d3f11bcc3` Graviton (ARM64): `sha256:174d7ab28b2f95e5309da80d95b88ad26f602dfe72c2b351a0ef9297a1412bfa`	Além das AMD64-based instâncias, a v1.2.0 agora também oferece suporte ARM64-based a instâncias. Incluída e verificada a compatibilidade com o Bottlerocket Compatível com o Kubernetes versão 1.27 Aprimoramentos gerais de performance e melhorias de estabilidade.	16 de junho de 2023	–

Versão do agente	Imagem do contêiner	Notas de atualização	Data de disponibilidade	Término do suporte[1] padrão
v1.1.0	`sha256:b19ba3a3c1a508d153263ae2fda891a7928b5ca9b3a5692db6c101829303281c`	Além do Versões do Kubernetes suportadas pelo agente de segurança GuardDuty, essa versão do agente também é compatível com a versão 1.26 do Kubernetes. Aprimoramentos gerais de performance e melhorias de estabilidade.	2 de maio de 2023	14 de maio de 2024
v1.0.0	`sha256:e38bdd2b1323e89113f1a31bd4bc8e5a8098525dd98e6981a28b9906b1e4411e`	Versão inicial do agente complementar do Amazon EKS.	30 de março de 2023	14 de maio de 2024

[1] Para obter informações sobre a atualização da versão atual do agente que está chegando ao fim do suporte padrão, consulteAtualização manual do agente de segurança para recursos do Amazon EKS.

Recursos adicionais – próximas etapas

Para obter mais informações sobre as próximas etapas, consulte os tópicos a seguir:

- Pré-requisitos para habilitar o Monitoramento de runtime – com as novas versões do agente, pode haver uma atualização na seção de pré-requisitos. Verifique e confirme se seus recursos atendem aos pré-requisitos mais recentes.
- Gerenciando agentes GuardDuty de segurança – ao gerenciar o agente manualmente, você é responsável por gerenciar as atualizações da versão do agente em execução em seus recursos. Com base no seu tipo de recurso (Amazon EKS ou Amazon EC2-Amazon ECS), execute as etapas para atualizar o agente de segurança. Além disso, valide sua configuração do endpoint da VPC.
- Analisando estatísticas de cobertura de runtime e solucionando problemas- Depois de atualizar o agente de segurança, você pode avaliar a cobertura do tempo de execução do seu recurso. Se houver algum problema de cobertura, use as etapas de solução de problemas associadas.

Desativação, desinstalação e remoção de recursos no Monitoramento de runtime

Esta seção se aplica Conta da AWS se você optar por desativar o Runtime Monitoring ou somente a configuração GuardDuty automatizada do agente para um tipo de recurso.

Desativando a configuração GuardDuty automatizada do agente

> GuardDuty não remove o agente de segurança que está implantado em seu recurso. No entanto, GuardDuty deixará de gerenciar as atualizações do agente de segurança.
>
> GuardDuty continua recebendo os eventos de tempo de execução do seu tipo de recurso. Para evitar um impacto nas estatísticas de uso, certifique-se de remover o agente de GuardDuty segurança do seu recurso.
>
> Se um usuário Conta da AWS usa ou não um VPC endpoint compartilhado, GuardDuty isso não exclui o VPC endpoint. Caso necessário, será preciso excluir o endpoint da VPC manualmente.

Como desativar o Monitoramento de runtime e o Monitoramento de runtime do EKS

> Esta seção se aplica aos seguintes cenários:

- O Monitoramento de runtime do EKS nunca foi habilitado de forma independente e agora o Monitoramento de runtime foi desabilitado.
- O Monitoramento de runtime e o Monitoramento de runtime EKS estão sendo desabilitados. Caso não tenha certeza sobre o status da configuração do Monitoramento de runtime do EKS, consulte Verificação do status da configuração do Monitoramento de runtime do EKS.

> **Como desabilitar o Monitoramento de runtime sem desabilitar o Monitoramento de runtime do EKS**
>
> Nesse cenário, em algum momento, o Monitoramento de runtime do EKS foi habilitado e, posteriormente, também foi habilitado o Monitoramento de runtime sem desabilitar o Monitoramento de runtime do EKS.
> Agora, ao desabilitar o Monitoramento de runtime, também será necessário desabilitar o Monitoramento de runtime do EKS; caso contrário, continuará incorrendo em custos de uso para o Monitoramento de runtime do EKS.

Se os cenários listados anteriormente se aplicarem a você, GuardDuty tomará as seguintes ações em sua conta:

- GuardDuty exclui o VPC endpoint que tem `GuardDutyManaged` a tag:. `true` Essa é a VPC criada para gerenciar o agente de segurança automatizado. GuardDuty
- GuardDuty exclui o grupo de segurança que foi marcado como`GuardDutyManaged:true`.
- Para uma VPC compartilhada que tenha sido usada por pelo menos uma conta participante, GuardDuty não exclui o VPC endpoint nem o grupo de segurança associado ao recurso de VPC compartilhado.
- Para um recurso do Amazon EKS, GuardDuty exclui o agente de segurança. Isso independe de ter sido gerenciado manualmente ou por meio de GuardDuty.

  Para um recurso do Amazon ECS, como uma tarefa do ECS é imutável, não é GuardDuty possível desinstalar o agente de segurança desse recurso. Isso independe de como você gerencia o agente de segurança — manual ou automaticamente GuardDuty. Depois de desativar o Runtime Monitoring, não GuardDuty anexará um contêiner auxiliar quando uma nova tarefa do ECS começar a ser executada. Para obter informações sobre como trabalhar com Fargate-ECS tarefas, consulteImplantação do agente de segurança no Amazon ECS no Fargate.

Para um recurso do Amazon EC2, GuardDuty desinstala o agente de segurança de todas as instâncias do Amazon EC2 gerenciadas pelo Systems Manager (SSM) somente quando ele atende às seguintes condições:

- Seu recurso não está marcado com`GuardDutyManaged`: `false` tag de exclusão.
- GuardDuty deve ter permissões para acessar as tags nos metadados da instância. Para esse recurso do EC2, a opção Acesso a tags nos metadados da instância foi definida como Permitir.

Ao interromper o gerenciamento manual do agente de segurança

Independentemente da abordagem usada para implantar e gerenciar o agente de GuardDuty segurança, para parar de monitorar os eventos de tempo de execução em seu recurso, você deve remover o agente GuardDuty de segurança. Para interromper o monitoramento dos eventos de runtime de um tipo de recurso em uma conta, também é possível excluir o endpoint do Amazon VPC.

Desinstalação manual do agente de segurança para recursos do Amazon EC2

Esta seção fornece métodos para desinstalar o agente GuardDuty de segurança dos seus recursos do Amazon EC2. Ao gerenciar o agente de segurança manualmente, você é responsável por remover o agente dos recursos. GuardDuty não executa nenhuma ação nos recursos que você gerencia.

Caso tenha criado um endpoint do Amazon VPC manualmente, depois de desinstalar o agente de segurança em todos os tipos de recursos monitorados em sua conta, é possível optar por excluir o endpoint da VPC. Trata-se de uma etapa distinta. Para obter mais informações, consulte To delete a VPC endpoint.

Considerando como o agente de segurança foi instalado em seu recurso, escolha um dos métodos a seguir para desinstalá-lo.

Tópicos

- Método 1 - Uso do comando Executar
- Método 2 - Uso de Gerenciadores de pacotes do Linux

Método 1 - Uso do comando Executar

Ao instalar o agente de segurança comMétodo 1 - Usando AWS Systems Manager, execute as seguintes etapas para desinstalar o agente:

Para desinstalar o agente GuardDuty de segurança

1. Você pode desinstalar o agente GuardDuty de segurança seguindo as etapas especificadas em AWS Systems Manager Executar comando no Guia do AWS Systems Manager usuário. Use a ação Desinstalar nos parâmetros para desinstalar o agente GuardDuty de segurança.

   Na seção Destinos, verifique se o impacto é apenas nas instâncias do Amazon EC2 das quais deseja desinstalar o agente de segurança.

   Use o seguinte GuardDuty documento e distribuidor:

   - Nome do documento: `AmazonGuardDuty-ConfigureRuntimeMonitoringSsmPlugin`
   - Distribuidor: `AmazonGuardDuty-RuntimeMonitoringSsmPlugin`
2. Depois de fornecer todos os detalhes, ao selecionar Executar, o agente de segurança que foi implantado nas instâncias do Amazon EC2 de destino será removido.

   Para remover a configuração do endpoint da Amazon VPC, deve-se desativar o Monitoramento de runtime e o Monitoramento de runtime do Amazon do EKS.
3. Caso também queira excluir o endpoint da VPC que está associado a esse agente de segurança, consulte To delete a VPC endpoint

Método 2 - Uso de Gerenciadores de pacotes do Linux

Ao instalar o agente de segurança comMétodo 2 - Usando Linux Package Managers, execute as seguintes etapas para desinstalar o agente:

Para desinstalar o agente GuardDuty de segurança

1. Conecte-se à sua instância. Para obter etapas sobre como proceder, consulte Conectar-se à sua instância Linux usando um cliente SSH no Guia do usuário do Amazon EC2.
2. Comando para desinstalar

   O comando a seguir desinstalará o agente de GuardDuty segurança da instância do Amazon EC2 à qual você se conecta:

- Para RPM:

```
sudo rpm -e amazon-guardduty-agent
```

- Para Debian:

```
sudo dpkg --purge amazon-guardduty-agent
```

Depois de executar o comando, também é possível verificar os logs associados a ele.

3. Caso também queira excluir o endpoint da VPC que está associado a esse agente de segurança, consulte To delete a VPC endpoint.

Desinstalando o agente de segurança para recursos do ECS-EC2 Bottlerocket

Execute as etapas a seguir para desinstalar o agente de GuardDuty segurança de suas instâncias do Bottlerocket ECS-EC2 .

Para desinstalar o agente GuardDuty de segurança

1. Para desinstalar o agente GuardDuty de segurança, use o comando AWS Systems Manager Executar (no Guia do AWS Systems Manager usuário) e defina o parâmetro de ação como Desinstalar.

   Na seção Metas, certifique-se de que o impacto seja somente nas instâncias do Bottlerocket das quais você deseja desinstalar o agente de segurança.

   Use o seguinte GuardDuty documento e distribuidor:

   - Nome do documento:`AmazonGuardDuty-ConfigureRuntimeMonitoringSsmPlugin`.
   - Distribuidor:`AmazonGuardDuty-RuntimeMonitoringSsmPlugin`.
2. Depois de fornecer todos os detalhes e escolher Executar, GuardDuty remove o agente de segurança das instâncias de destino do Bottlerocket.
3. Para excluir também o VPC endpoint associado a esse agente de segurança, consulte. To delete a VPC endpoint

Como remover os recursos do agente de segurança

Esta seção explica como você pode limpar os AWS recursos associados ao agente de segurança. Conforme listado emDesativação, desinstalação e remoção de recursos, não GuardDuty excluirá nem removerá todos os recursos do agente de segurança. A seção a seguir fornece instruções sobre como se pode excluir os recursos do agente de segurança.

Para excluir o endpoint da Amazon VPC

Ao administrar o agente de segurança manualmente, é possível que um endpoint do Amazon VPC tenha sido criado manualmente. Depois de desinstalar o agente de segurança de todos os recursos monitorados em sua conta, pode-se optar por excluir esse endpoint da VPC.

A lista a seguir apresenta cenários em que o uso de uma VPC compartilhada é comparado ao não uso de uma VPC compartilhada.

- Sem uma VPC compartilhada: quando não quiser mais monitorar um recurso em uma conta, considere a possibilidade de excluir o endpoint do Amazon VPC.
- Com uma VPC compartilhada - Quando uma conta proprietária de VPC compartilhada exclui o recurso de VPC compartilhada que ainda estava sendo usado, o status de cobertura do Monitoramento de runtime (e, quando aplicável, do Monitoramento de runtime do EKS) para os recursos na sua conta proprietária de VPC compartilhada e na conta participante pode se tornar não íntegro. Para obter informações sobre status de cobertura, consulte Analisando estatísticas de cobertura de runtime e solucionando problemas.

Para excluir o endpoint da VPC, consulte Excluir um endpoint de interface no AWS PrivateLink Guia.

Para excluir o grupo de segurança

- Sem uma VPC compartilhada: quando não quiser mais monitorar um tipo de recurso em uma conta, considere a possibilidade de excluir o grupo de segurança associado à Amazon VPC.
- Com uma VPC compartilhada - Quando a conta proprietária da VPC compartilhada exclui o grupo de segurança, qualquer conta participante que estiver usando atualmente o grupo de segurança associado à VPC compartilhada, o status de cobertura do Monitoramento de runtime para os recursos na conta proprietária da VPC compartilhada e a conta participante podem se tornar não íntegros. Para obter mais informações, consulte Analisando estatísticas de cobertura de runtime e solucionando problemas.

Para obter mais informações sobre as etapas, consulte Excluir grupos de segurança do Amazon EC2 no Guia do usuário do Amazon EC2.

Para remover o agente de GuardDuty segurança de um cluster EKS

Para remover o agente de segurança do seu cluster do EKS que não deseja mais monitorar, consulte Como remover um complemento do Amazon EKS de um cluster no Guia do usuário do Amazon EKS.

A remoção do agente complementar do EKS não remove o namespace `amazon-guardduty` do cluster do EKS. Para excluir o namespace `amazon-guardduty`, consulte Deleting a namespace.

Excluir o **`amazon-guardduty`** namespace (cluster do EKS)

Desabilitar o gerenciamento automático do agente GuardDuty não remove automaticamente o `amazon-guardduty` namespace do seu cluster do EKS. Para excluir o namespace `amazon-guardduty`, consulte Deleting a namespace.

GuardDuty Proteção contra malware para EC2

A Proteção contra malware para o EC2 ajuda a detectar a possível presença de um malware ao examinar os volumes do Amazon Elastic Block Store (Amazon EBS) que são anexados às instâncias do Amazon Elastic Compute Cloud (Amazon EC2) e workloads de contêiner executados no Amazon EC2. A Proteção contra malware para o EC2 fornece opções de verificação nas quais é possível decidir se deseja incluir ou excluir instâncias específicas do Amazon EC2 no momento da verificação. Ele também oferece a opção de reter os snapshots dos volumes do Amazon EBS anexados às instâncias do Amazon EC2 ou às cargas de trabalho de contêineres em suas contas. GuardDuty Os snapshots são retidos somente quando o malware é encontrado e as descobertas da Proteção contra malware para o EC2 são geradas.

A Proteção contra malware para o EC2 foi projetada de forma a não afetar o desempenho de seus recursos. Para obter informações sobre como funciona a Proteção contra Malware para EC2 GuardDuty, consulteComo GuardDuty escaneia volumes do EBS em busca de detecção de malware. Para obter informações sobre a disponibilidade da Proteção contra Malware para EC2 em diferentes Regiões da AWS, consulteRegiões e endpoints.

> **Observações**
>
> A Proteção contra malware para EC2 oferece suporte a verificações de malware em instâncias gerenciadas para o Modo Automático do Amazon EKS. Para obter mais informações, consulte Suporte a instâncias gerenciadas no Guardduty.
> O Malware Protection for EC2 não oferece suporte a escaneamentos de malware para AWS Fargate cargas de trabalho executadas com o Amazon EKS ou o Amazon ECS.
> Para ter mais informações sobre recursos do Amazon EKS, consulte O que é o Amazon EKS? no Guia do usuário do Amazon EKS.

Tópicos

- Comparando a verificação de GuardDuty-initiated malware e a verificação de On-demand malware
- Como GuardDuty escaneia volumes do EBS em busca de detecção de malware
- Volumes Amazon EBS compatíveis para verificação de malware
- Configurar a retenção de snapshots e a cobertura de verificação do EC2
- GuardDuty-initiated escaneamento de malware
- On-demand escaneamento de malware em GuardDuty

- Monitoramento de status e resultados de verificações na Proteção contra Malware para o EC2
- GuardDuty contas de serviço por Região da AWS
- Cotas na Proteção contra malware para o EC2

Comparando a verificação de GuardDuty-initiated malware e a verificação de On-demand malware

O Malware Protection for EC2 oferece dois tipos de escaneamento para detectar atividades potencialmente maliciosas em suas instâncias e cargas de trabalho de contêineres do Amazon EC2 GuardDuty-initiated : escaneamento de malware e escaneamento de malware. On-demand A tabela a seguir mostra a comparação entre os dois tipos de verificação.

Factor	GuardDuty-initiated escaneamento de malware	On-demand escaneamento de malware
Como a verificação é invocada	Depois de ativar a verificação de GuardDuty-initiated malware, sempre que GuardDuty gerar uma descoberta que indique a presença potencial de malware em uma instância do Amazon EC2 ou em uma carga de trabalho de contêiner, inicia GuardDuty automaticamente uma verificação de malware sem agente nos volumes do Amazon EBS anexados ao seu recurso potencialmente afetado. Para obter mais informações, consulte GuardDuty-initiated escaneamento de malware.	Você pode iniciar uma verificação de On-demand malware fornecendo o Amazon Resource Name (ARN) da sua instância do Amazon EC2. Você pode iniciar uma verificação de On-demand malware mesmo quando nenhuma GuardDuty descoberta for gerada para seu recurso. Para obter mais informações, consulte On-demand escaneamento de malware em GuardDuty.
Configuração necessária	Para usar a verificação de GuardDuty-initiated malware,	Sua conta deve estar GuardDuty ativada. Para usar

Factor	GuardDuty-initiated escaneamento de malware	On-demand escaneamento de malware
	você deve habilitá-la em sua conta. Para gerenciar várias contas usando AWS Organizations nosso método baseado em convite, consulteHabilitando a verificação de GuardDuty-initiated malware em ambientes com várias contas. Para ativar a verificação de GuardDuty-initiated malware em sua própria conta, consulteAtivando a verificação de GuardDuty-initiated malware para uma conta independente.	a verificação de On-demand malware, não há necessidade de configuração no nível do recurso.
Tempo de espera para iniciar uma nova verificação	Sempre que GuardDuty gera um delesDescobertas que invocam a verificação de GuardDuty-initiated malware, uma verificação de malware é iniciada automaticamente apenas uma vez a cada 24 horas.	Você pode iniciar uma verificação de On-demand malware no mesmo recurso a qualquer momento após 1 hora a partir da hora de início da verificação anterior.

Factor	GuardDuty-initiated escaneamento de malware	On-demand escaneamento de malware
Disponibilidade do período de teste gratuito de 30 dias [1]	Ao ativar a verificação de GuardDuty-initiated malware pela primeira vez em sua conta, você pode usar um período de teste gratuito de 30 dias. Para obter mais informaçõ es, consulte Teste gratuito de 30 dias na verificação de GuardDuty-initiated malware.	Não há período de teste gratuito com a verificação de On-demand malware para GuardDuty contas novas ou existentes.
Opções de verificação[2]	Depois de configurar a verificação de GuardDuty-initiated malware, o Malware Protection for EC2 oferece a opção de verificar ou ignorar recursos específicos do Amazon EC2 usando tags. A Proteção contra malware para o EC2 não iniciará uma verificação automática dos recursos que foram excluídos da verificação. Para obter mais informações, consulte Opções de verificação com tags definidas pelo usuário.	Como o recurso ARN é fornecido para iniciar manualmente uma verificaç ão de malware sob demanda, o uso de Opções de verificaç ão com tags definidas pelo usuário não se aplica.

[1]Incorrerá em custos de uso para criar snapshots de volumes EBS e reter snapshots.. Para obter mais informações sobre como configurar sua conta para reter snapshots, consulte Retenção de snapshots

[2] Tanto GuardDuty-initiated o escaneamento de On-demand malware quanto o escaneamento de malware suportam o uso de uma tag global para excluir recursos do Amazon EC2 dos

escaneamentos de malware. Para obter mais informações, consulte Tag `GuardDutyExcluded` global.

Como GuardDuty escaneia volumes do EBS em busca de detecção de malware

Esta seção explica como o Malware Protection for EC2, incluindo tanto GuardDuty-initiated o escaneamento quanto o escaneamento de On-demand malware, verifica os volumes do Amazon EBS associados às suas instâncias e cargas de trabalho de contêineres do Amazon EC2. Antes de continuar, considere as seguintes personalizações:

- Opções de verificação: a Proteção contra malware para o EC2 oferece a capacidade de especificar tags para incluir ou excluir instâncias do Amazon EC2 e volumes do Amazon EBS do processo de verificação. Somente o escaneamento de GuardDuty-initiated malware suporta opções de escaneamento com tags definidas pelo usuário. Tanto GuardDuty-initiated o escaneamento de On-demand malware quanto o escaneamento de malware suportam a `GuardDutyExcluded` tag global. Para obter mais informações, consulte Opções de verificação com tags definidas pelo usuário.
- Retenção de snapshots — A proteção contra malware para EC2 oferece uma opção para reter os snapshots dos volumes do Amazon EBS em sua conta. AWS Essa configuração está desativada por padrão. Você pode optar pela retenção de instantâneos para escaneamentos de malware GuardDuty iniciados e sob demanda. Para obter mais informações, consulte Retenção de snapshots.

Quando GuardDuty gera uma ou maisDescobertas que invocam a verificação de GuardDuty-initiated malware, essa atividade será um motivo GuardDuty para iniciar uma verificação de malware. Se suas opções de escaneamento não excluírem essa instância, então GuardDuty iniciará o escaneamento.

Para iniciar uma verificação de On-demand malware nos volumes do Amazon EBS associados a uma instância do Amazon EC2, forneça o Amazon Resource Name (ARN) da instância do Amazon EC2.

Como resposta ao início de uma verificação de malware sob demanda ou uma verificação automática de GuardDuty-initiated malware, GuardDuty cria instantâneos dos volumes relevantes do EBS anexados ao recurso potencialmente afetado e os compartilha com o. GuardDuty conta de serviço Ao GuardDuty criar um snapshot dos seus volumes do EBS, ele adiciona uma tag padrão chamada. `GuardDutyScanId` Essa tag ajuda GuardDuty a acessar o instantâneo. Não remova essa

tag. A partir desses instantâneos, GuardDuty cria uma réplica criptografada do volume do EBS na conta de serviço.

Após a conclusão da verificação, GuardDuty exclui os volumes de réplica criptografados do EBS e os instantâneos dos seus volumes do EBS. Como padrão, a configuração de retenção de snapshots permanece desabilitada. No entanto, os snapshots são retidos se o bloqueio de snapshots do Amazon EBS estiver habilitado para eles, independentemente dos resultados e das configurações da verificação. GuardDuty não é possível modificar as configurações de bloqueio do snapshot do Amazon EBS.

A lista a seguir descreve o comportamento de retenção de snapshots, independentemente do bloqueio de snapshots do EBS:

A retenção de snapshots está ativada:

- Quando o malware é encontrado, GuardDuty retém os instantâneos em seu. Conta da AWS
- Quando nenhum malware é encontrado, GuardDuty não retém os instantâneos, a menos que estejam bloqueados.

A retenção de snapshots permanece desabilitada (configuração padrão):

- Independentemente de o malware ser encontrado ou não, os snapshots não são retidos.
- GuardDuty não é possível excluir snapshots bloqueados do Amazon EBS.

GuardDuty reterá cada volume de réplica do EBS na conta de serviço por até 55 horas. Se houver uma interrupção ou falha no serviço com uma réplica do volume do EBS e sua verificação de malware, esse volume do EBS GuardDuty será retido por no máximo sete dias. O período estendido de retenção de volume serve para fazer a triagem e resolver a interrupção ou falha. GuardDuty O Malware Protection for EC2 excluirá os volumes de réplica do EBS da conta de serviço após a interrupção ou falha ser resolvida, ou quando o período de retenção estendido expirar.

Para obter informações sobre a metodologia de detecção de GuardDuty malware e os mecanismos de verificação que ela usa, consulteGuardDuty mecanismo de verificação de detecção de malware.

Volumes Amazon EBS compatíveis para verificação de malware

Em todos os Regiões da AWS locais onde há GuardDuty suporte ao recurso Malware Protection for EC2, você pode escanear os volumes do Amazon EBS que não estão criptografados ou não estão criptografados. É possível ter volumes do Amazon EBS criptografados com uma Chave gerenciada

pela AWSou com a chave gerenciada pelo cliente. Atualmente, algumas das regiões em que a Proteção contra malware para o EC2 está disponível podem oferecer suporte às duas formas de criptografar seus volumes do Amazon EBS, enquanto outras oferecem suporte somente à chave gerenciada pelo cliente. Para obter informações sobre as regiões compatíveis, consulte GuardDuty contas de serviço por Região da AWS. Para obter informações sobre regiões onde GuardDuty está disponível, mas a Proteção contra Malware para EC2 não está disponível, consulteRegion-specific disponibilidade de recursos.

A lista a seguir descreve a chave que GuardDuty usa se seus volumes do Amazon EBS estão criptografados ou não:

- Volumes do Amazon EBS que não são criptografados ou criptografados com Chave gerenciada pela AWS — GuardDuty usam sua própria chave para criptografar os volumes de réplica do Amazon EBS.

  Se sua região não permitir a verificação de volumes do Amazon EBS que são criptografados com a criptografia do Amazon EBS por padrão, será preciso modificar a chave padrão para que se torne uma chave gerenciada pelo cliente. Isso ajudará a GuardDuty acessar esses volumes do EBS. Ao modificar a chave, até mesmo os volumes futuros do EBS serão criados com a chave atualizada para que ela GuardDuty possa suportar escaneamentos de malware. Para saber as etapas de modificação da chave padrão, consulte Modificar padrão AWS KMS ID da chave de um volume do Amazon EBS a próxima seção.
- Volumes do Amazon EBS que são criptografados com chave gerenciada pelo cliente — GuardDuty usam a mesma chave para criptografar o volume de réplica do EBS. Para obter informações sobre quais políticas relacionadas à AWS KMS criptografia são suportadas, consulteService-linked permissões de função para proteção contra malware para EC2.

Modificar padrão AWS KMS ID da chave de um volume do Amazon EBS

Quando você cria um volume do Amazon EBS usando a criptografia do Amazon EBS e não especifica o ID da AWS KMS chave, seu volume do Amazon EBS é criptografado com uma chave padrão para criptografia. Ao habilitar a criptografia por padrão, o Amazon EBS criptografará automaticamente novos volumes e snapshots usando sua chave KMS padrão para a criptografia do Amazon EBS.

É possível modificar a chave de criptografia padrão e usar uma chave gerenciada pelo cliente para a criptografia do Amazon EBS. Isso ajudará a GuardDuty acessar esses volumes do Amazon EBS. Para modificar o ID da chave padrão do EBS, adicione a seguinte permissão necessária à sua

política do IAM: `ec2:modifyEbsDefaultKmsKeyId`. Qualquer volume recém-criado do Amazon EBS que venha a ser criptografado, mas que não especifique um ID de chave KMS associado, usará o ID de chave padrão. Use um dos métodos a seguir para atualizar o ID da chave padrão do EBS:

Para modificar o ID da chave do KMS padrão de um volume do Amazon EBS

Execute um destes procedimentos:

- Usando uma API — Você pode usar a ModifyEbsDefaultKmsKeyIdAPI. Para obter informações sobre como é possível visualizar o status de criptografia do seu volume, consulte Criar volume do Amazon EBS.
- Usando o AWS CLI comando — O exemplo a seguir modifica a ID da chave KMS padrão que criptografará os volumes do Amazon EBS se você não fornecer uma ID da chave KMS. Certifique-se de substituir a região pelo ID Região da AWS da sua chave KM.

  ```
  aws ec2 modify-ebs-default-kms-key-id --region us-west-2 --kms-key-
  id AKIAIOSFODNN7EXAMPLE
  ```

  O comando acima gerará uma saída semelhante à seguinte saída:

  ```
  {
    "KmsKeyId": "arn:aws:kms:us-west-2:444455556666:key/AKIAIOSFODNN7EXAMPLE"
  }
  ```

  Para obter mais informações, consulte modify-ebs-default-kms-key-id.

Configurar a retenção de snapshots e a cobertura de verificação do EC2

Esta seção explica como personalizar as opções de verificação de malware para suas instâncias do Amazon EC2. Essas personalizações se aplicam tanto à verificação de On-demand malware quanto às iniciadas por. GuardDuty Você pode fazer o seguinte:

- Habilitar retenção de snapshots — Quando habilitado antes de um escaneamento, GuardDuty reterá o snapshot do Amazon EBS que foi GuardDuty detectado como malicioso.
- Escolha quais instâncias do Amazon EC2 verificar – Use tags para incluir ou excluir instâncias específicas do Amazon EC2 das verificações de malware.

Retenção de snapshots

GuardDuty oferece a opção de reter os instantâneos dos volumes do EBS em sua AWS conta. Como padrão, a configuração de retenção de snapshots permanece desabilitada. Os snapshots só serão retidos se você tiver essa configuração habilitada antes do início da verificação.

Quando a verificação é iniciada, GuardDuty gera os volumes de réplica do EBS com base nos instantâneos dos seus volumes do EBS. Depois que a verificação for concluída e a configuração de retenção de snapshots em sua conta já estiver habilitada, os snapshots dos seus volumes do EBS serão retidos somente quando o malware for encontrado e as Tipos de descoberta da Proteção contra malware para EC2 forem geradas. Quando nenhum malware é encontrado, independentemente de suas configurações de snapshot, ele exclui GuardDuty automaticamente os snapshots de seus volumes do EBS, a menos que o bloqueio de snapshots do Amazon EBS tenha sido ativado nos snapshots criados.

Custo de uso de snapshots

Durante a verificação de malware, à medida que GuardDuty cria os snapshots dos seus volumes do Amazon EBS, há um custo de uso associado a essa etapa. Se você habilitar a configuração de retenção de snapshots em sua conta, quando o malware for encontrado e os snapshots forem retidos, você incorrerá no custo de uso do mesmo. Para obter informações sobre o custo dos snapshots e sua retenção, consulte os preços do Amazon EBS.

Como conta de GuardDuty administrador delegado, somente você pode fazer essa atualização em nome das contas dos membros da organização. No entanto, se a conta de um membro for gerenciada pelo método de convite, ele poderá fazer essa alteração sozinho. Para obter mais informações, consulte Relações entre administradores do Macie e contas de membros.

Escolha seu método de acesso preferido para habilitar a configuração de retenção de snapshots.

Console

1. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.
2. No painel de navegação, em Planos de proteção, selecione Proteção contra malware para o EC2.
3. Selecione Configurações gerais na seção inferior do console. Para reter os snapshots, ative a Retenção de snapshots.

API/CLI

Execute UpdateMalwareScanSettingspara atualizar a configuração atual da configuração de retenção de instantâneos.

Como alternativa, você pode executar o AWS CLI comando a seguir para reter automaticamente os instantâneos quando o GuardDuty Malware Protection for EC2 gerar descobertas.

Certifique-se de *detector-id* substituí-lo por seu próprio válidodetectorId.

Para encontrar a opção detectorId para sua conta e região atual, consulte a página de configurações no https://console.aws.amazon.com/guardduty/console ou execute a ListDetectorsAPI.

```
aws guardduty update-malware-scan-settings --detector-
id 60b87779336485625 54d637e0e4bb3b2 --ebs-snapshot-preservation
 "RETENTION_WITH_FINDING"
```

Se você quiser desabilitar a retenção de snapshots, substitua RETENTION_WITH_FINDING por NO_RETENTION.

Opções de verificação com tags definidas pelo usuário

Ao usar a verificação de GuardDuty-initiated malware, você também pode especificar tags para incluir ou excluir instâncias do Amazon EC2 e volumes do Amazon EBS do processo de verificação e detecção de ameaças. Você pode personalizar cada escaneamento de GuardDuty-initiated malware editando as tags na lista de tags de inclusão ou exclusão. Cada lista pode incluir até 50 tags.

Caso ainda não tenha tags definidas pelo usuário associadas aos seus recursos do EC2, consulte Marcar seus recursos do Amazon EC2 no Guia do usuário do Amazon EC2..

> **Note**
>
> On-demand o escaneamento de malware não suporta opções de escaneamento com tags definidas pelo usuário. Ele oferece suporte à Tag GuardDutyExcluded global.

Para excluir instâncias do EC2 da verificação de malware

Se você quiser excluir qualquer instância do Amazon EC2 ou volume do Amazon EBS durante o processo de digitalização, você pode definir a `GuardDutyExcluded` tag `true` para qualquer instância do Amazon EC2 ou volume do Amazon EBS e não a digitalizará. GuardDuty Para obter mais informações sobre a tag `GuardDutyExcluded`, consulte Service-linked permissões de função para proteção contra malware para EC2. Também é possível pode adicionar uma tag de instância do Amazon EC2 a uma lista de exclusão. Se você adicionar várias tags à lista de tags de exclusão, qualquer instância do Amazon EC2 que contenha pelo menos uma dessas tags será excluída do processo de verificação de malware.

Como conta de GuardDuty administrador delegado, somente você pode fazer essa atualização em nome das contas dos membros da organização. No entanto, se a conta de um membro for gerenciada pelo método de convite, ele poderá fazer essa alteração sozinho. Para obter mais informações, consulte Relações entre administradores do Macie e contas de membros.

Selecione seu método de acesso preferido para adicionar uma tag associada a uma instância do Amazon EC2 a uma lista de exclusão.

Console

1. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.
2. No painel de navegação, em Planos de proteção, selecione Proteção contra malware para o EC2.
3. Expanda a seção de Inclusion/Exclusion tags. Selecione Adicionar tags.
4. Selecione Tags de exclusão e, em seguida, selecione Confirmar.
5. Especifique o par de **`Key`**-**`Value`** da tag que você deseja excluir. É opcional fornecer o **`Value`**. Depois de adicionar todas as tags, escolha Salvar.

   > **Important**
   >
   > As chaves e os valores de marcas diferenciam maiúsculas de minúsculas. Para obter mais informações, consulte Restrições de tags no Guia do usuário do Amazon EC2.

   Se um valor para uma chave não for fornecido e a instância do EC2 for marcada com a chave especificada, essa instância do EC2 será excluída do processo de verificação de GuardDuty-initiated malware, independentemente do valor atribuído à tag.

API/CLI

Execute UpdateMalwareScanSettingsexcluindo uma instância do EC2 ou uma carga de trabalho de contêiner do processo de digitalização.

O comando de AWS CLI exemplo a seguir adiciona uma nova tag à lista de tags de exclusão. Substitua o *detector-id* de exemplo por seu próprio `detectorId` válido.

`MapEquals` é uma lista de pares de `Key`/`Value`.

Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no https://console.aws.amazon.com/guardduty/console ou execute a ListDetectorsAPI.

```
aws guardduty update-malware-scan-settings --detector-
id 60b87779336485625 54d637e0e4bb3b2 --scan-resource-criteria '{"Exclude":
 {"EC2_INSTANCE_TAG" : {"MapEquals": [{ "Key": "TestKeyWithValue", "Value":
 "TestValue" }, {"Key":"TestKeyWithoutValue"} ]}}}' --ebs-snapshot-preservation
 "RETENTION_WITH_FINDING"
```

> **Important**
>
> As chaves e os valores de marcas diferenciam maiúsculas de minúsculas. Para obter mais informações, consulte Restrições de tags no Guia do usuário do Amazon EC2.

Para incluir instâncias do EC2 na verificação de malware

Se quiser verificar uma instância do EC2, adicione sua tag à lista de inclusão. Ao adicionar uma tag a uma lista de tags de inclusão, uma instância do EC2 que não contém nenhuma das tags adicionadas é ignorada na verificação de malware. Se você adicionar várias tags à lista de tags de inclusão, uma instância do EC2 que contenha pelo menos uma dessas tags será incluída na verificação de malware. Às vezes, uma instância do EC2 pode ser ignorada durante o processo de verificação por outras razões. Para obter mais informações, consulte Razões para ignorar o recurso durante a verificação de malware.

Como conta de GuardDuty administrador delegado, somente você pode fazer essa atualização em nome das contas dos membros da organização. No entanto, se a conta de um membro for gerenciada pelo método de convite, ele poderá fazer essa alteração sozinho. Para obter mais informações, consulte Relações entre administradores do Macie e contas de membros.

Escolha seu método de acesso preferido para adicionar uma tag associada a uma instância do Amazon EC2 a uma lista de exclusão.

Console

1. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.
2. No painel de navegação, em Planos de proteção, selecione Proteção contra malware para o EC2.
3. Expanda a seção de Inclusion/Exclusion tags. Selecione Adicionar tags.
4. Escolha Tags de inclusão e, em seguida, Confirmar.
5. Escolha Adicionar nova tag de inclusão e especifique o par de **`Key`**-**`Value`** que deseja incluir. É opcional fornecer o **`Value`**.

   Depois de adicionar todas as tags de inclusão, escolha Salvar.

   Se o valor de uma chave não for fornecido e uma instância do EC2 for marcada com a chave especificada, a instância do EC2 será incluída no processo de verificação da Proteção contra malware para o EC2, independentemente do valor atribuído à tag.

API/CLI

- Execute UpdateMalwareScanSettingspara incluir uma instância do EC2 ou uma carga de trabalho de contêiner no processo de digitalização.

  O comando de AWS CLI exemplo a seguir adiciona uma nova tag à lista de tags de inclusão. Certifique-se de substituir o exemplo *`detector-id`* pelo seu próprio exemplo válido`detectorId`. Substitua o exemplo *`TestKey`* e *`TestValue`* pelo `Value` par `Key` e da tag associada ao seu recurso do EC2.

  `MapEquals` é uma lista de pares de `Key`/`Value`.

  Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no https://console.aws.amazon.com/guardduty/console ou execute a ListDetectorsAPI.

```
aws guardduty update-malware-scan-settings --detector-
id 60b87779336485625 54d637e0e4bb3b2 --scan-resource-criteria '{"Include":
 {"EC2_INSTANCE_TAG" : {"MapEquals": [{ "Key": "TestKeyWithValue", "Value":
```

```
"TestValue" }, {"Key":"TestKeyWithoutValue"} ]}}}' --ebs-snapshot-preservation
"RETENTION_WITH_FINDING"
```

> **Important**
>
> As chaves e os valores de marcas diferenciam maiúsculas de minúsculas. Para obter mais informações, consulte Restrições de tags no Guia do usuário do Amazon EC2.

> **Note**
>
> Pode levar até 5 minutos GuardDuty para detectar uma nova etiqueta.

A qualquer momento, você pode escolher tags de inclusão ou tags de exclusão, mas não ambas. Se quiser alternar entre as tags, escolha essa tag no menu suspenso ao adicionar novas tags e Confirme sua seleção. Essa ação limpa todas as suas tags atuais.

Tag **`GuardDutyExcluded`** global

GuardDuty usa uma chave de tag global,`GuardDutyExcluded`, que você pode adicionar aos seus recursos do Amazon EC2 e definir o valor da tag como. `true` Esse recurso do Amazon EC2 que possui esse par de chave e valor de tag será excluído da verificação de malware. Ambos os tipos de escaneamento (GuardDuty-initiated escaneamento de On-demand malware e escaneamento de malware) suportam a tag global. Caso seja iniciada uma verificação de malware sob demanda em um Amazon EC2, será gerada uma ID de verificação. No entanto, a verificação será ignorada por uma `EXCLUDED_BY_SCAN_SETTINGS` razão. Para obter mais informações, consulte Razões para ignorar o recurso durante a verificação de malware.

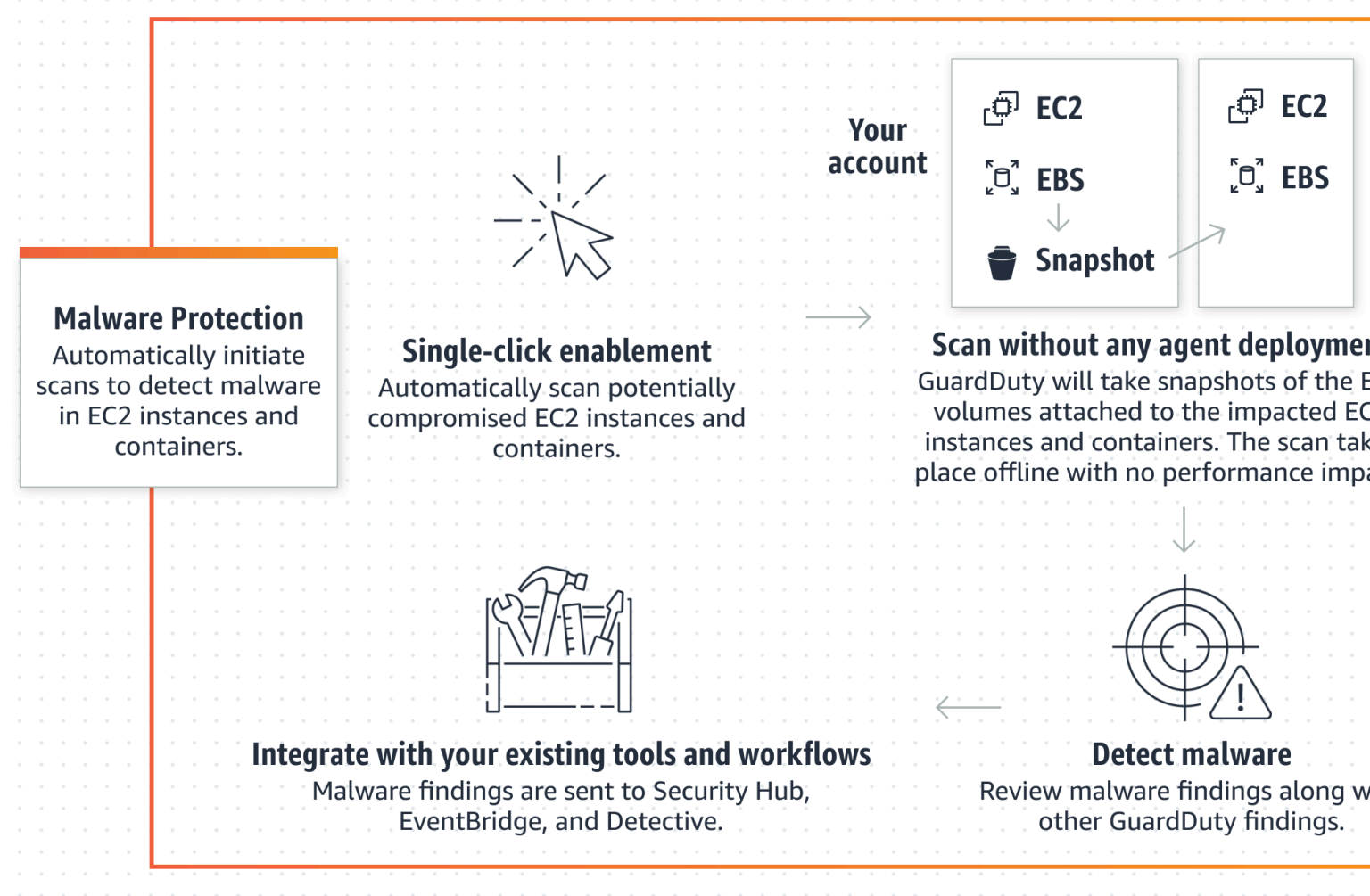
GuardDuty-initiated escaneamento de malware

Com a verificação de GuardDuty-initiated malware ativada, sempre que GuardDuty geradaDescobertas que invocam a verificação de GuardDuty-initiated malware, uma verificação de malware sem agente nos volumes do Amazon Elastic Block Store (Amazon EBS) anexados ao recurso potencialmente afetado do Amazon EC2 será iniciada. Antes de iniciar uma verificação, deve-se preparar a conta para quaisquer personalizações. Com as opções de verificação, pode-se adicionar tags de inclusão associadas aos recursos que se deseja verificar ou adicionar tags de exclusão associadas aos recursos que se deseja ignorar do processo de verificação. O início

automático do escaneamento sempre considerará suas opções de escaneamento. GuardDuty também suporta um par global`GuardDutyExcluded`: `true` tag chave:valor. Quando você adiciona essa tag global a um recurso do Amazon EC2, inicia a verificação e, GuardDuty em seguida, a ignora. Também é possível optar por ativar a configuração de retenção de snapshots para reter os snapshots dos volumes EBS em que o malware foi possivelmente detectado. Para obter mais informações sobre opções de verificação, tag de exclusão global e configurações de snapshot, consulte Configurar a retenção de snapshots e a cobertura de verificação do EC2

Ao GuardDuty gerar várias descobertas para o mesmo recurso do Amazon EC2, GuardDuty será possível iniciar uma verificação somente após 24 horas desde a última GuardDuty-initiated verificação de malware. Para obter informações sobre como os volumes do Amazon EBS anexados à sua instância do Amazon EC2 ou workload do contêiner são verificados, consulte Como GuardDuty escaneia volumes do EBS em busca de detecção de malware.

A imagem a seguir descreve como a verificação de GuardDuty-initiated malware funciona.



Para obter informações sobre a metodologia de detecção de GuardDuty malware e os mecanismos de verificação que ela usa, consulteGuardDuty mecanismo de verificação de detecção de malware.

Quando o malware é encontrado, é GuardDuty geradoTipos de descoberta da Proteção contra malware para EC2. Se GuardDuty não gerar uma descoberta indicativa de malware no mesmo recurso, nenhuma verificação de GuardDuty-initiated malware será invocada. Você também pode iniciar uma verificação de On-demand malware no mesmo recurso. Para obter mais informações, consulte On-demand escaneamento de malware em GuardDuty.

Teste gratuito de 30 dias na verificação de GuardDuty-initiated malware

Você pode optar por ativar ou desativar a verificação de GuardDuty-initiated malware Conta da AWS em um servidor compatível Região da AWS a qualquer momento. Caso tenha uma organização, cada conta de membro tem sua própria avaliação gratuita de 30 dias.

Para entender como funciona a avaliação gratuita de 30 dias, considere os seguintes cenários:

- Quando você ativa GuardDuty pela primeira vez (nova GuardDuty conta), a verificação de GuardDuty-initiated malware também é ativada e incluída no teste gratuito de 30 dias associado ao GuardDuty serviço.
- Uma GuardDuty conta existente pode ativar a verificação de GuardDuty-initiated malware pela primeira vez com um teste gratuito de 30 dias. Ao habilitar esse recurso em uma região diferente pela primeira vez, uma avaliação gratuita de 30 dias será concedida nessa região.
- Se você já usou o Malware Protection for EC2 Região da AWS antes de esse plano de proteção ser dividido em dois tipos de escaneamento — escaneamento de GuardDuty-initiated malware e escaneamento de On-demand malware, você pode continuar usando o escaneamento de GuardDuty-initiated malware com o mesmo modelo de preços e o mesmo Região da AWS. Se você ativar a verificação de GuardDuty-initiated malware pela primeira vez em uma nova região, sua conta receberá um teste gratuito de 30 dias.

> **Note**
>
> Mesmo que esteja em um período de avaliação gratuita de 30 dias, aplica-se os custos de uso padrão para a criação de snapshots de volume do Amazon EBS e sua retenção. Para obter mais informações, consulte Definição de preço do Amazon EBS.

Habilitando a verificação de GuardDuty-initiated malware em ambientes com várias contas

Em um ambiente de várias contas, somente a conta de GuardDuty administrador pode habilitar a verificação de GuardDuty-initiated malware em nome de suas contas de membros. Além disso, uma conta de administrador que gerencia as contas dos membros com AWS Organizations suporte pode optar por ativar automaticamente a verificação de GuardDuty-initiated malware em todas as contas novas e existentes na organização. Para obter mais informações, consulte Gerenciando GuardDuty contas com AWS Organizations.

Estabelecendo acesso confiável para permitir a verificação de GuardDuty-initiated malware

Se a conta de administrador GuardDuty delegado não for igual à conta de gerenciamento em sua organização, a conta de gerenciamento deverá habilitar a verificação de GuardDuty-initiated malware em sua organização. Dessa forma, a conta de administrador delegado pode criar contas de Service-linked permissões de função para proteção contra malware para EC2 membros que são gerenciadas por meio AWS Organizations de.

> **Note**
>
> Antes de designar uma conta de GuardDuty administrador delegado, consulte. Considerações e recomendações

Escolha seu método de acesso preferido para permitir que a conta do GuardDuty administrador delegado habilite a verificação de GuardDuty-initiated malware nas contas dos membros da organização.

Console

1. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.

   Para fazer login, use a conta de gerenciamento AWS Organizations da sua organização.

2. a. Se você não designou uma conta de GuardDuty administrador delegado, então:

      Na página Configurações, em Conta de GuardDuty administrador delegado, insira os 12 dígitos **`account ID`** que você deseja designar para administrar a GuardDuty política em sua organização. Selecione Delegar.

b. i. Se você já designou uma conta de GuardDuty administrador delegado diferente da conta de gerenciamento, então:

Na página Configurações, em Administrador delegado, ative a configuração Permissões. Essa ação permitirá que a conta do GuardDuty administrador delegado anexe permissões relevantes às contas dos membros e habilite a verificação de GuardDuty-initiated malware nessas contas dos membros.

ii. Se você já designou uma conta de GuardDuty administrador delegado que é igual à conta de gerenciamento, você pode ativar diretamente a verificação de GuardDuty-initiated malware para as contas dos membros. Para obter mais informações, consulte Auto-enable GuardDuty-initiated verificação de malware para todas as contas de membros.

> **Tip**
>
> Se a conta do GuardDuty administrador delegado for diferente da sua conta de gerenciamento, você deverá fornecer permissões à conta do GuardDuty administrador delegado para permitir a verificação de GuardDuty-initiated malware nas contas dos membros.

3. Se você quiser permitir que a conta de GuardDuty administrador delegado habilite a verificação de GuardDuty-initiated malware para contas de membros em outras regiões, altere a sua Região da AWS e repita as etapas acima.

API/CLI

1. Usando as credenciais da conta de gerenciamento, execute o seguinte comando:

```
aws organizations enable-aws-service-access --service-principal malware-
protection.guardduty.amazonaws.com
```

2. (Opcional) para ativar a verificação de GuardDuty-initiated malware para a conta de gerenciamento que não é uma conta de administrador delegado, a conta de gerenciamento primeiro criará o código Service-linked permissões de função para proteção contra malware para EC2 explicitamente em sua conta e, em seguida, habilitará a verificação de GuardDuty-initiated malware a partir da conta de administrador delegado, semelhante a qualquer outra conta de membro.

```
aws iam create-service-linked-role --aws-service-name malware-
protection.guardduty.amazonaws.com
```

3. Você designou a conta de GuardDuty administrador delegado na conta atualmente selecionada Região da AWS. Se você designou uma conta como conta de GuardDuty administrador delegado em uma região, essa conta deverá ser sua conta de GuardDuty administrador delegado em todas as outras regiões. Repita a etapa acima para todas as outras regiões.

Configurando a verificação de GuardDuty-initiated malware para uma conta de administrador delegado GuardDuty

Escolha seu método de acesso preferido para ativar ou desativar a verificação de GuardDuty-initiated malware para uma conta de GuardDuty administrador delegado.

Console

1. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.
2. No painel de navegação, selecione Proteção contra malware para o EC2.
3. Na página Proteção contra malware para EC2, escolha Editar ao lado da verificação de GuardDuty-initiated malware.
4. Execute um destes procedimentos:

   Utilizar Ativar para todas as contas

   - Escolha Habilitar para todas as contas. Isso habilitará o plano de proteção para todas as GuardDuty contas ativas em sua AWS organização, incluindo as novas contas que ingressam na organização.
   - Escolha Salvar.

   Utilizar Configurar contas manualmente

   - Para habilitar o plano de proteção somente para a conta de GuardDuty administrador delegado, escolha Configurar contas manualmente.
   - Escolha Habilitar na seção Conta de GuardDuty administrador delegado (esta conta).
   - Escolha Salvar.

API/CLI

Execute a operação da API updateDetector usando seu próprio ID de detector regional e transmitindo o `name` do objeto `features` como `EBS_MALWARE_PROTECTION` e `status` como`ENABLED`.

Você pode ativar a verificação de GuardDuty-initiated malware executando o AWS CLI comando a seguir. Certifique-se de usar a conta de GuardDuty administrador delegado válida*detector ID*.

Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no https://console.aws.amazon.com/guardduty/console ou execute a ListDetectorsAPI.

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 /
              --account-ids 555555555555 /
              --features '[{"Name": "EBS_MALWARE_PROTECTION", "Status": "ENABLED"}]'
```

Auto-enable GuardDuty-initiated verificação de malware para todas as contas de membros

Escolha seu método de acesso preferido para ativar o recurso de verificação de GuardDuty-initiated malware para todas as contas dos membros. Isso inclui contas-membro existentes e as novas contas que ingressam na organização.

Console

1. Faça login no Console de gerenciamento da AWS e abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.

   Certifique-se de usar as credenciais da conta de GuardDuty administrador delegado.
2. Execute um destes procedimentos:

   Usar o Proteção contra malware para o EC2 page

   1. No painel de navegação, selecione Proteção contra malware para o EC2.
   2. Na página Proteção contra malware para EC2, escolha Editar na seção de verificação de GuardDuty-initiated malware.
   3. Escolha Habilitar para todas as contas. Essa ação ativa automaticamente a verificação de GuardDuty-initiated malware para contas novas e existentes na organização.

4. Escolha Salvar.

> **Note**
>
> Pode levar até 24 horas para atualizar a configuração das contas-membro.

Usar o Contas page

1. No painel de navegação, selecione Contas.
2. Na página Contas, escolha Auto-enableas preferências antes de Adicionar contas por convite.
3. Na janela Gerenciar preferências de ativação automática, escolha Habilitar para todas as contas na verificação de GuardDuty-initiated malware.
4. Na página Proteção contra malware para EC2, escolha Editar na seção de verificação de GuardDuty-initiated malware.
5. Escolha Habilitar para todas as contas. Essa ação ativa automaticamente a verificação de GuardDuty-initiated malware para contas novas e existentes na organização.
6. Escolha Salvar.

> **Note**
>
> Pode levar até 24 horas para atualizar a configuração das contas-membro.

Usar o Contas page

1. No painel de navegação, selecione Contas.
2. Na página Contas, escolha Auto-enableas preferências antes de Adicionar contas por convite.
3. Na janela Gerenciar preferências de ativação automática, escolha Habilitar para todas as contas na verificação de GuardDuty-initiated malware.
4. Escolha Salvar.

Se você não conseguir usar a opção Habilitar para todas as contas, consulte Ative seletivamente a verificação de GuardDuty-initiated malware para contas de membros.

API/CLI

- Para ativar seletivamente a verificação de GuardDuty-initiated malware em suas contas de membros, invoque a operação da updateMemberDetectorsAPI usando a sua própria. *detector ID*
- O exemplo a seguir mostra como você pode ativar a verificação de GuardDuty-initiated malware para uma única conta de membro. Para desabilitar uma conta de membro, substitua `ENABLED` por `DISABLED`.

  Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no https://console.aws.amazon.com/guardduty/console ou execute a ListDetectorsAPI.

  ```
  aws guardduty update-member-detectors --detector-
  id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features
   '[{"Name": "EBS_MALWARE_PROTECTION", "Status": "ENABLED"}]'
  ```

  Também é possível passar uma lista de IDs de conta separados por um espaço.
- Quando o código é executado com êxito, ele retorna uma lista vazia de `UnprocessedAccounts`. Se houver algum problema na alteração das configurações do detector de uma conta, esse ID de conta será listado junto com um resumo do problema.

Ative a verificação de GuardDuty-initiated malware para todas as contas de membros ativas existentes

Escolha seu método de acesso preferido para permitir a verificação de GuardDuty-initiated malware em todas as contas de membros ativos existentes na organização.

Para configurar a verificação de GuardDuty-initiated malware para todas as contas de membros ativas existentes

1. Faça login no Console de gerenciamento da AWS e abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.

   Faça login usando as credenciais da conta de GuardDuty administrador delegado.
2. No painel de navegação, selecione Proteção contra malware para o EC2.
3. No Malware Protection for EC2, você pode ver o status atual da configuração do escaneamento de GuardDuty-initiated malware. Na seção Contas-membro ativas, escolha Ações.

4. No menu suspenso Ações, escolha Habilitar para todas as contas-membro ativas existentes.
5. Escolha Salvar.

Auto-enable GuardDuty-initiated verificação de malware para contas de novos membros

As contas de membros recém-adicionadas devem ser ativadas GuardDuty antes de selecionar a configuração da verificação de GuardDuty-initiated malware. As contas dos membros gerenciadas por convite podem configurar manualmente a verificação de GuardDuty-initiated malware em suas contas. Para obter mais informações, consulte Step 3 - Accept an invitation.

Escolha seu método de acesso preferido para permitir a verificação de GuardDuty-initiated malware em novas contas que ingressam na sua organização.

Console

A conta de GuardDuty administrador delegado pode habilitar a verificação de GuardDuty-initiated malware para novas contas membros em uma organização, usando a página Proteção contra malware para EC2 ou Contas.

Para ativar automaticamente a verificação de GuardDuty-initiated malware para contas de novos membros

1. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.

   Certifique-se de usar as credenciais da conta de GuardDuty administrador delegado.
2. Execute um destes procedimentos:
   - Página de como usar a Proteção contra malware para o EC2:
     1. No painel de navegação, selecione Proteção contra malware para o EC2.
     2. Na página Proteção contra malware para EC2, escolha Editar na verificação de GuardDuty-initiated malware.
     3. Escolha Configurar contas manualmente.
     4. Selecione Habilitar automaticamente para novas contas-membro. Essa etapa garante que, sempre que uma nova conta ingressar na sua organização, a verificação de GuardDuty-initiated malware seja ativada automaticamente para a conta dessa pessoa. Somente a conta do GuardDuty administrador delegado da organização pode modificar essa configuração.
     5. Escolha Salvar.

- Como usar a página Contas:

  1. No painel de navegação, selecione Contas.
  2. Na página Contas, escolha Auto-enablepreferências.
  3. Na janela Gerenciar preferências de ativação automática, selecione Ativar para novas contas na verificação de GuardDuty-initiated malware.
  4. Escolha Salvar.

API/CLI

- Para ativar ou desativar a verificação de GuardDuty-initiated malware para novas contas de membros, invoque a operação da UpdateOrganizationConfigurationAPI usando a sua própria*`detector ID`*.
- O exemplo a seguir mostra como você pode ativar a verificação de GuardDuty-initiated malware para uma única conta de membro. Para desabilitá-lo, consulte Ative seletivamente a verificação de GuardDuty-initiated malware para contas de membros. Se não quiser habilitá-lo para todas as novas contas que ingressarem na organização, defina `AutoEnable` como `NONE`.

  Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no https://console.aws.amazon.com/guardduty/console ou execute a ListDetectorsAPI.

  ```
  aws guardduty update-organization-configuration --detector-
  id 12abc34d567e8fa901bc2d34e56789f0 --AutoEnable --features '[{"Name":
   "EBS_MALWARE_PROTECTION", "AutoEnable": NEW}]'
  ```

  Também é possível passar uma lista de IDs de conta separados por um espaço.
- Quando o código é executado com êxito, ele retorna uma lista vazia de `UnprocessedAccounts`. Se houver algum problema na alteração das configurações do detector de uma conta, esse ID de conta será listado junto com um resumo do problema.

Ative seletivamente a verificação de GuardDuty-initiated malware para contas de membros

Escolha seu método de acesso preferido para configurar seletivamente a verificação de GuardDuty-initiated malware para contas de membros.

Console

1. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.
2. No painel de navegação, selecione Contas.
3. Na página Contas, revise a coluna de verificação de GuardDuty-initiated malware para ver o status da sua conta de membro.
4. Selecione a conta para a qual você deseja configurar a verificação de GuardDuty-initiated malware. Você pode selecionar várias contas ao mesmo tempo.
5. No menu Editar planos de proteção, escolha a opção apropriada para a verificação de GuardDuty-initiated malware.

API/CLI

Para ativar ou desativar seletivamente a verificação de GuardDuty-initiated malware em suas contas de membros, invoque a operação da updateMemberDetectorsAPI usando a sua própria. *detector ID*

O exemplo a seguir mostra como você pode ativar a verificação de GuardDuty-initiated malware para uma única conta de membro.

Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no https://console.aws.amazon.com/guardduty/console ou execute a ListDetectorsAPI.

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --account-ids 111122223333 --features '[{"Name": "EBS_MALWARE_PROTECTION",
 "Status": "ENABLED"}]'
```

Também é possível passar uma lista de IDs de conta separados por um espaço.

Quando o código é executado com êxito, ele retorna uma lista vazia de `UnprocessedAccounts`. Se houver algum problema na alteração das configurações do detector de uma conta, esse ID de conta será listado junto com um resumo do problema.

Para ativar seletivamente a verificação de GuardDuty-initiated malware em suas contas de membros, execute a operação da updateMemberDetectorsAPI usando a sua própria*detector ID*. O exemplo a seguir mostra como você pode ativar a verificação de GuardDuty-initiated malware para uma única conta de membro.

Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no https://console.aws.amazon.com/guardduty/console ou execute a ListDetectorsAPI.

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --account-ids 111122223333 --data-sources '{"MalwareProtection":
{"ScanEc2InstanceWithFindings":{"EbsVolumes":true}}}'
```

Também é possível passar uma lista de IDs de conta separados por um espaço.

Quando o código é executado com êxito, ele retorna uma lista vazia de `UnprocessedAccounts`. Se houver algum problema na alteração das configurações do detector de uma conta, esse ID de conta será listado junto com um resumo do problema.

Ative a verificação de GuardDuty-initiated malware para contas existentes na organização gerenciadas por meio de convite

A proteção contra GuardDuty malware para a função vinculada ao serviço (SLR) do EC2 deve ser criada nas contas dos membros. A conta do administrador não pode ativar o recurso de verificação de GuardDuty-initiated malware em contas de membros que não são gerenciadas pelo AWS Organizations.

Atualmente, você pode executar as etapas a seguir por meio do GuardDuty console em https://console.aws.amazon.com/guardduty/para habilitar a verificação de GuardDuty-initiated malware nas contas de membros existentes.

Console

1. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.

   Faça login usando suas credenciais de conta do administrador.
2. No painel de navegação, selecione Contas.
3. Selecione a conta de membro para a qual você deseja ativar a verificação de GuardDuty-initiated malware. Você pode selecionar várias contas ao mesmo tempo.
4. Escolha Ações.
5. Selecione Desassociar membro.
6. Na sua conta-membro, escolha Proteção contra malware em Planos de proteção no painel de navegação.

7. Escolha Ativar verificação de GuardDuty-initiated malware. GuardDuty criará uma SLR para a conta do membro. Para obter mais informações sobre a SLR, consulte Service-linked permissões de função para proteção contra malware para EC2.
8. Na sua conta de administrador, selecione Contas no painel de navegação.
9. Escolha a conta-membro que precisa ser adicionada novamente à organização.
10. Escolha Ações e selecione Adicionar membro.

API/CLI

1. Use a conta de administrador para executar a DisassociateMembersAPI nas contas de membros que desejam ativar a verificação de GuardDuty-initiated malware.
2. Use sua conta de membro para invocar e ativar UpdateDetectora verificação de GuardDuty-initiated malware.

   Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no https://console.aws.amazon.com/guardduty/console ou execute a ListDetectorsAPI.

   ```
   aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0
    --data-sources '{"MalwareProtection":{"ScanEc2InstanceWithFindings":
   {"EbsVolumes":true}}}'
   ```
3. Use a conta de administrador para executar a API CreateMembers e adicionar o membro de volta à organização.

Ativando a verificação de GuardDuty-initiated malware para uma conta independente

Uma conta autônoma é responsável pela decisão de ativar ou desativar um plano de proteção Conta da AWS em uma conta específica Região da AWS.

Se sua conta estiver associada a uma conta de GuardDuty administrador por meio AWS Organizations ou pelo método de convite, esta seção não se aplica à sua conta. Para obter mais informações, consulte Habilitando a verificação de GuardDuty-initiated malware em ambientes com várias contas.

Depois de ativar a verificação de GuardDuty-initiated malware, GuardDuty iniciará uma verificação de malware do volume do Amazon EBS que está conectado à instância do Amazon EC2 que estava envolvida em um. GuardDuty Para obter uma lista das descobertas que iniciam a verificação de malware, consulte Descobertas que invocam a verificação de GuardDuty-initiated malware.

Escolha seu método de acesso preferido para configurar a verificação de GuardDuty-initiated malware para uma conta independente.

Console

1. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.
2. No painel de navegação, em Planos de proteção, selecione Proteção contra malware para o EC2.
3. O painel Proteção contra malware para EC2 lista o status atual da verificação de GuardDuty-initiated malware em sua conta. Escolha Ativar para ativar a verificação de GuardDuty-initiated malware nessa conta.
4. Selecione Salvar para confirmar sua seleção.

API/CLI

Execute a operação da API updateDetector usando seu próprio ID de detector regional e transmitindo o objeto `dataSources` com `EbsVolumes` definido como `true`.

Você também pode ativar a verificação de GuardDuty-initiated malware AWS CLI usando o AWS CLI comando a seguir. Certifique-se de usar seu próprio válido*`detector ID`*.

Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no https://console.aws.amazon.com/guardduty/console ou execute a ListDetectorsAPI.

```
 aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
features [{"Name" : "EBS_MALWARE_PROTECTION", "Status" : "ENABLED"}]'
```

Descobertas que invocam a verificação de GuardDuty-initiated malware

Quando GuardDuty detecta um comportamento suspeito que é indicativo de malware em uma instância do Amazon EC2 ou uma carga de trabalho de contêiner que está sendo executada em

uma instância do Amazon EC2, gerará uma descoberta. GuardDuty Se essa descoberta gerada pertencer à lista de GuardDuty descobertas a seguir, GuardDuty iniciará automaticamente a verificação de malware nos volumes do Amazon EBS anexados à instância do Amazon EC2 envolvida na descoberta. Após a verificação, se GuardDuty detectar malware, ele também gerará um ou maisTipos de descoberta da Proteção contra malware para EC2.

Se alguma das seguintes GuardDuty descobertas for gerada em sua conta, GuardDuty iniciará automaticamente a verificação de malware no volume do Amazon EBS da instância potencialmente comprometida do Amazon EC2.

- Backdoor:EC2/C&CActivity.B
- Backdoor:EC2/C&CActivity.B!DNS
- Backdoor:EC2/DenialOfService.Dns
- Backdoor:EC2/DenialOfService.Tcp
- Backdoor:EC2/DenialOfService.Udp
- Backdoor:EC2/DenialOfService.UdpOnTcpPorts
- Backdoor:EC2/DenialOfService.UnusualProtocol
- Backdoor:EC2/Spambot
- CryptoCurrency:EC2/BitcoinTool.B
- CryptoCurrency:EC2/BitcoinTool.B!DNS
- DefenseEvasion:Runtime/PtraceAntiDebugging
- DefenseEvasion:Runtime/SuspiciousCommand
- Execution:Runtime/MaliciousFileExecuted
- Execution:Runtime/MaliciousFileExecuted.Custom
- Execution:Runtime/SuspiciousCommand
- Execution:Runtime/SuspiciousShellCreated
- Execution:Runtime/SuspiciousTool
- Impact:EC2/AbusedDomainRequest.Reputation
- Impact:EC2/BitcoinDomainRequest.Reputation
- Impact:EC2/MaliciousDomainRequest.Reputation
- Impact:EC2/PortSweep

- Impact:EC2/SuspiciousDomainRequest.Reputation
- Impact:EC2/WinRMBruteForce (Somente de saída)
- PrivilegeEscalation:Runtime/ElevationToRoot
- Recon:EC2/Portscan
- Trojan:EC2/BlackholeTraffic
- Trojan:EC2/BlackholeTraffic!DNS
- Trojan:EC2/DGADomainRequest.B
- Trojan:EC2/DGADomainRequest.C!DNS
- Trojan:EC2/DNSDataExfiltration
- Trojan:EC2/DriveBySourceTraffic!DNS
- Trojan:EC2/DropPoint
- Trojan:EC2/DropPoint!DNS
- Trojan:EC2/PhishingDomainRequest!DNS
- UnauthorizedAccess:EC2/RDPBruteForce (Somente de saída)
- UnauthorizedAccess:EC2/SSHBruteForce (Somente de saída)
- UnauthorizedAccess:EC2/TorClient
- UnauthorizedAccess:EC2/TorRelay
- Backdoor:Runtime/C&CActivity.B
- Backdoor:Runtime/C&CActivity.B! DNS
- CryptoCurrency:Runtime/BitcoinTool.B
- CryptoCurrency:Runtime/BitcoinTool.B! DNS
- Execution:Runtime/NewBinaryExecuted
- Execution:Runtime/NewLibraryLoaded
- Execution:Runtime/ReverseShell
- Impact:Runtime/AbusedDomainRequest.Reputation
- Impact:Runtime/BitcoinDomainRequest.Reputation
- Impact:Runtime/CryptoMinerExecuted
- Impact:Runtime/MaliciousDomainRequest.Reputation

- Impact:Runtime/SuspiciousDomainRequest.Reputation
- PrivilegeEscalation:Runtime/CGroupsReleaseAgentModified
- PrivilegeEscalation:Runtime/ContainerMountsHostDirectory
- PrivilegeEscalation:Runtime/DockerSocketAccessed
- PrivilegeEscalation:Runtime/RuncContainerEscape
- PrivilegeEscalation:Runtime/UserfaultfdUsage
- Trojan:Runtime/BlackholeTraffic
- Trojan:Runtime/BlackholeTraffic! DNS
- Trojan:Runtime/DropPoint
- Trojan:Runtime/DropPoint! DNS
- Trojan:Runtime/DGADomainRequest.C! DNS
- Trojan:Runtime/DriveBySourceTraffic! DNS
- Trojan:Runtime/PhishingDomainRequest! DNS
- UnauthorizedAccess:Runtime/MetadataDNSRebind

On-demand escaneamento de malware em GuardDuty

On-demand a verificação de malware ajuda você a detectar a presença de malware nos volumes do Amazon Elastic Block Store (Amazon EBS) anexados às suas instâncias do Amazon EC2. Sem necessidade de configuração, é possível iniciar uma verificação de malware sob demanda fornecendo o nome do recurso da Amazon (ARN) da instância do Amazon EC2 que deseja verificar. Você pode iniciar uma verificação de malware sob demanda por meio do GuardDuty console ou da API. Antes de iniciar uma verificação de malware sob demanda, defina sua configuração de Retenção de snapshots preferencial. Os cenários a seguir podem ajudá-lo a identificar quando usar o tipo de verificação de On-demand malware com GuardDuty:

- Você deseja detectar a presença de malware em suas instâncias do Amazon EC2 sem ativar a verificação de GuardDuty-initiated malware.
- Você ativou a verificação de GuardDuty-initiated malware e uma verificação foi invocada automaticamente. Depois de seguir a correção recomendada para o tipo de descoberta gerada pela Proteção contra Malware para o EC2, caso queira iniciar uma verificação no mesmo recurso, inicie uma verificação de malware sob demanda após 1 hora do horário de início da verificação anterior.

On-demand a verificação de malware não exige que tenham passado 24 horas desde o início da verificação de malware anterior. Deveria ter passado uma hora antes de iniciar uma verificação de On-demand malware no mesmo recurso. Para evitar a duplicação de uma verificação de malware na mesma instância do EC2, consulte Re-scanning instância do Amazon EC2 escaneada anteriormente.

> **Note**
>
> On-demand a verificação de malware não está incluída no período de teste gratuito de 30 dias com GuardDuty. O custo de uso se aplica ao volume total do Amazon EBS verificado para cada verificação de malware. Para obter mais informações, consulte os GuardDuty preços da Amazon. Para obter informações sobre os custos de criação dos snapshots de volumes do Amazon EBS e sua retenção, consulte Definição de preços do Amazon EBS.

Como funciona a verificação de On-demand malware

Com a verificação de On-demand malware, você pode iniciar uma solicitação de verificação de malware para sua instância do Amazon EC2 mesmo quando ela estiver em uso no momento. Depois de iniciar uma verificação de On-demand malware, GuardDuty cria instantâneos dos volumes do Amazon EBS anexados à instância do Amazon EC2 cujo Amazon Resource Name (ARN) foi fornecido para a verificação. Em seguida, GuardDuty compartilha esses instantâneos com o. GuardDuty conta de serviço GuardDuty cria volumes de réplica criptografados do EBS a partir desses snapshots na conta de serviço. GuardDuty Para obter mais informações sobre como os volumes do Amazon EBS são verificados, consulte Como GuardDuty escaneia volumes do EBS em busca de detecção de malware.

> **Note**
>
> GuardDuty cria os instantâneos dos dados que já foram gravados nos volumes do Amazon EBS no momento em que você inicia uma verificação de malware. On-demand

Se um malware for encontrado e você tiver ativado a configuração de retenção de instantâneos, os instantâneos do seu volume do EBS serão automaticamente retidos no seu. Conta da AWS On-demand o escaneamento de malware gera Tipos de descoberta da Proteção contra malware para

EC2 o. Se o malware não for encontrado, independentemente da configuração de retenção de snapshots, os snapshots dos seus volumes do EBS serão excluídos.

GuardDuty usa uma chave de tag global,`GuardDutyExcluded`, que você pode adicionar aos seus recursos do Amazon EC2 e definir o valor da tag como. `true` Esse recurso do Amazon EC2 que possui esse par de chave e valor de tag será excluído da verificação de malware. Ambos os tipos de escaneamento (GuardDuty-initiated escaneamento de On-demand malware e escaneamento de malware) suportam a tag global. Caso seja iniciada uma verificação de malware sob demanda em um Amazon EC2, será gerada uma ID de verificação. No entanto, a verificação será ignorada por uma `EXCLUDED_BY_SCAN_SETTINGS` razão. Para obter mais informações, consulte Razões para ignorar o recurso durante a verificação de malware.

Iniciando a verificação de On-demand malware em GuardDuty

Esta seção fornece uma lista de pré-requisitos antes de iniciar uma verificação de malware sob demanda e as etapas para iniciar a verificação em um recurso pela primeira vez.

Como conta de GuardDuty administrador, você pode iniciar uma verificação de malware sob demanda em nome de suas contas de membros ativas que tenham os seguintes pré-requisitos configurados em suas contas. Contas autônomas e contas de membros ativos também GuardDuty podem iniciar uma verificação de malware sob demanda para suas próprias instâncias do Amazon EC2.

Pré-requisitos

Antes de iniciar uma verificação de On-demand malware, sua conta deve atender aos seguintes pré-requisitos:

- GuardDuty deve estar habilitado no Regiões da AWS local em que você deseja iniciar a verificação de malware sob demanda.
- Verifique se a AWS política gerenciada: AmazonGuardDutyFullAccess_v2 (recomendado) está anexada ao usuário do IAM ou ao perfil do IAM. Você precisará da chave de acesso e da chave secreta associadas ao usuário do IAM ou ao perfil do IAM.
- Como conta de GuardDuty administrador delegado, você tem a opção de iniciar uma verificação de malware sob demanda em nome de uma conta de membro ativa.
- Antes de iniciar uma verificação de malware sob demanda, confirme se nenhuma outra verificação foi iniciada no mesmo recurso na última 1 hora; caso contrário, ela será eliminada. Para obter mais informações, consulte Re-scanning instância do Amazon EC2 escaneada anteriormente.

- Caso sua conta de membro não possua as Service-linked permissões de função para proteção contra malware para EC2, iniciar uma varredura de malware sob demanda para uma instância do Amazon EC2 que pertença à sua conta criará automaticamente o SLR para a Proteção contra Malware para o EC2.

> **Important**
>
> Verifique se ninguém excluiu as permissões SLR para Proteção contra malware para o EC2 quando a verificação de malware ainda estiver em andamento. Essa verificação de malware pode ser iniciada GuardDuty ou iniciada sob demanda. A exclusão do SLR impedirá que a varredura seja concluída com êxito e fornecerá um resultado definitivo.

Inicie a verificação de On-demand malware

Você pode iniciar uma verificação de malware sob demanda em sua conta por meio GuardDuty do console ou usando AWS CLI. Será preciso fornecer o nome do recurso da Amazon (ARN) para o Amazon EC2 para o qual deseja iniciar a verificação. As etapas detalhadas são fornecidas no console e nas AWS CLI instruções da API/A na seção a seguir.

Selecione seu método de acesso preferencial para iniciar uma verificação de malware sob demanda.

Console

1. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.
2. Inicie a verificação usando uma das seguintes opções:
   a. Página sobre como usar a Proteção contra malware para o EC2:
      i. No painel de navegação, em Planos de proteção, selecione Proteção contra malware para o EC2.
      ii. Na página Proteção contra malware para o EC2, forneça o ARN da instância do Amazon EC2[1] para o qual deseja iniciar a verificação.
   b. Como usar a página Verificações de malware:
      i. No painel de navegação, escolha Verificações de malware.
      ii. Selecione Iniciar verificação sob demanda e forneça o ARN da instância do Amazon EC2[1] para o qual deseja iniciar a verificação.

iii. Se for uma nova verificação, selecione um ID de instância do Amazon EC2 na página Verificações de malware.

Expanda a lista suspensa Iniciar escaneamento sob demanda e escolha Re-scan a instância selecionada.

3. Depois de iniciar uma verificação com sucesso usando qualquer um dos métodos, um ID de verificação é gerado. Você pode usar esse ID de verificação para acompanhar o andamento da verificação. Para obter mais informações, consulte Monitoramento de status e resultados de verificação de malware.

API/CLI

Invoke StartMalwareScanthat aceita a instância[1] `resourceArn` do Amazon EC2 para a qual você deseja iniciar uma verificação de malware sob demanda.

```
aws guardduty start-malware-scan --resource-arn "arn:aws:ec2:us-
east-1:555555555555:instance/i-b188560f"
```

Depois de iniciar uma verificação com sucesso, `StartMalwareScan` retorna um `scanId`. Invoque e DescribeMalwareScansmonitore o progresso da verificação iniciada.

[1]Para obter informações sobre o formato do ARN da sua instância do Amazon EC2, consulte Nomes de recurso da Amazon (ARN). Para instâncias do Amazon EC2, você pode usar o seguinte exemplo de formato de ARN substituindo os valores da partição, região, ID da Conta da AWS e ID de instância do Amazon EC2. Para obter informações sobre o tamanho do ID da sua instância, consulte IDs de recursos.

```
arn:aws:ec2:us-east-1:555555555555:instance/i-b188560f
```

AWS Organizations política de controle de serviços — Acesso negado

Usando as políticas de controle de serviços (SCPs) em AWS Organizations, a conta do GuardDuty administrador delegado pode restringir permissões e negar ações, como iniciar uma verificação de malware sob demanda para a instância do Amazon EC2 de propriedade de suas contas.

Como conta GuardDuty membro, ao iniciar uma verificação de malware sob demanda para suas instâncias do Amazon EC2, você pode receber uma mensagem de erro. Você pode se conectar à

conta de gerenciamento para entender por que um SCP foi configurado para sua conta de membro. Para obter mais informações, consulte Efeitos do SCP sobre as permissões.

Re-scanning instância do Amazon EC2 escaneada anteriormente

Independentemente de uma verificação ser feita GuardDuty-initiated ou iniciada sob demanda, você pode iniciar uma nova verificação de malware sob demanda na mesma instância do Amazon EC2 após 1 hora a partir da hora de início da verificação de malware anterior. Caso a nova verificação de malware seja iniciada em até 1 hora após o início da verificação de malware anterior, sua solicitação resultará no seguinte erro, e nenhum ID de verificação será gerado para essa solicitação.

```
A scan was started on this resource recently. You can request a scan on the same resource one hour after the previous scan start time.
```

As etapas para verificar novamente a instância permanecem as mesmas usadas para iniciar uma verificação de malware sob demanda pela primeira vez. Para obter informações sobre as etapas, consulte Inicie a verificação de On-demand malware.

Para acompanhar o status das verificações de malware, consulte Monitoramento de status e resultados de verificações na Proteção contra Malware para o EC2.

Monitoramento de status e resultados de verificações na Proteção contra Malware para o EC2

Depois que uma verificação de malware é iniciada em uma instância do Amazon EC2, GuardDuty fornece automaticamente os campos de status e resultado. Você pode monitorar o status por meio de transições e ver se o malware foi detectado. A tabela a seguir fornece os valores possíveis associados à verificação de malware.

Valores potenciais
`Running`, `Completed` , `Skipped` ou `Failed`
`Clean` ou `Infected`

Valores potenciais
`GuardDuty initiated` ou `On demand`

* O resultado da verificação é preenchido somente quando o status dela se torna `Completed`. O resultado da verificação `Infected` significa que GuardDuty detectou a presença de malware.

Os resultados de verificação de cada verificação de malware têm um período de retenção de 90 dias. Escolha seu método de acesso preferido para rastrear o status da verificação de malware.

Console

1. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.
2. No painel de navegação, escolha Verificações de malware do EC2.
3. Você pode filtrar as verificações de malware pelas seguintes Propriedades disponíveis na barra de pesquisa de filtro.
   - ID da verificação – identificador exclusivo associado à verificação de malware do EC2.
   - ID da conta — Conta da AWS ID em que a verificação de malware foi iniciada.
   - ARN da instância do EC2 – nome do recurso da Amazon (ARN) associado à instância do Amazon EC2 associada à verificação.
   - Status da verificação – o status da verificação do volume do EBS, como Em execução, Ignorado e Concluído
   - Tipo de escaneamento — Indica se foi um escaneamento de On-demand malware ou um escaneamento de GuardDuty-initiated malware.

API/CLI

- Depois que a verificação de malware tiver um resultado de verificação, use DescribeMalwareScanspara filtrar as varreduras de malware

com base em EC2_INSTANCE_ARNSCAN_ID,ACCOUNT_ID, SCAN_TYPEGUARDDUTY_FINDING_ID,SCAN_STATUS, e. SCAN_START_TIME

Os critérios do GUARDDUTY_FINDING_ID filtro estão disponíveis quando o SCAN_TYPE é GuardDuty iniciado.

- Você pode alterar o exemplo *filter-criteria* no comando abaixo. Atualmente, você pode filtrar com base em uma CriterionKey de cada vez. As opções para CriterionKey são EC2_INSTANCE_ARN, SCAN_ID, ACCOUNT_ID, SCAN_TYPE GUARDDUTY_FINDING_ID, SCAN_STATUS e SCAN_START_TIME.

  Você pode alterar o *max-results* (até 50) e *sort-criteria* o. O AttributeName é obrigatório e deve ser scanStartTime.

  No exemplo a seguir, os valores em *red* são espaços reservados. Substitua-os pelos valores apropriados para sua conta. Por exemplo, substitua o exemplo detector-id *60b87779336485625 54d637e0e4bb3b2* pelo seu próprio válidodetector-id. Se você usar o CriterionKey mesmo exemplo abaixo, certifique-se de substituir o exemplo EqualsValue pelo seu próprio válido AWS *scan-id*.

  ```
  aws guardduty describe-malware-scans --detector-
  id 60b87779336485625 54d637e0e4bb3b2 --max-results 1 --sort-criteria
   '{"AttributeName": "scanStartTime", "OrderBy": "DESC"}' --filter-criteria
   '{"FilterCriterion":[{"CriterionKey":"SCAN_ID", "FilterCondition":
  {"EqualsValue":"123456789012"}}] }'
  ```

- A resposta desse comando exibe no máximo um resultado com detalhes sobre o recurso afetado e as descobertas de malware (se Infected).

GuardDuty contas de serviço por Região da AWS

Quando um snapshot é criado e compartilhado com uma conta GuardDuty de serviço, um novo evento é criado em seus CloudTrail registros. Esse evento especifica o snapshotId e userId (conta GuardDuty de serviço correspondente Região da AWS). Para obter mais informações, consulte Como GuardDuty escaneia volumes do EBS em busca de detecção de malware.

O exemplo a seguir é um trecho de um CloudTrail evento que mostra o corpo da solicitação: ModifySnapshotAttribute

```
"requestParameters": {
```

```
        "snapshotId": "snap-1234567890abcdef0",
        "createVolumePermission": {
            "add": {
                "items": [
                    {
                        "userId": "111122223333"
                    }
                ]
            }
        },
        "attributeType": "CREATE_VOLUME_PERMISSION"
    }
```

A tabela a seguir mostra as contas GuardDuty de serviço de cada região. `userId`É a conta GuardDuty de serviço e depende da região selecionada.

Região da AWS	Código da região	GuardDuty ID da conta de serviço (**`userId`**)
Leste dos EUA (Norte da Virgínia)	us-east-1	652050842985
Leste dos EUA (Ohio)	us-east-2	178123968615
Oeste dos EUA (N. da Califórnia)	us-west-1	669213148797
Oeste dos EUA (Oregon)	us-west-2	447226417196
Ásia-Pacífico (Mumbai)	ap-south-1	913179291432
Ásia-Pacífico (Osaka)	ap-northeast-3	089661699081
Ásia-Pacífico (Seul)	ap-northeast-2	039163547507
Ásia-Pacífico (Tóquio)	ap-northeast-1	874749492622
Ásia-Pacífico (Singapura)	ap-southeast-1	247460962669
Ásia-Pacífico (Sydney)	ap-southeast-2	124839743349

Região da AWS	Código da região	GuardDuty ID da conta de serviço (**`userId`**)
Canadá (Central)	ca-central-1	175877067165
Oeste do Canadá (Calgary)	ca-west-1	894794104037
Europa (Frankfurt)	eu-central-1	00:294, 50.712
Europa (Irlanda)	eu-west-1	283769539786
Europa (Londres)	eu-west-2	310125036783
Europa (Paris)	eu-west-3	866607715269
Europa (Estocolmo)	eu-north-1	693780578038
China (Pequim)	cn-north-1	448721096076
China (Ningxia)	cn-northwest-1	480864352451
América do Sul (São Paulo)	sa-east-1	546914126324
Ásia-Pacífico (Hyderabad) (Opt-in)	ap-south-2	682251015962
Ásia-Pacífico (Melbourne) (Opt-in)	ap-southeast-4	353488359550
Ásia-Pacífico (Malásia) Opt-in ()	ap-southeast-5	009160069308
Ásia-Pacífico (Tailândia) Opt-in ()	ap-southeast-7	941377115582
Europa (Espanha) (Opt-in)	eu-south-2	936182149045
Europa (Zurique) (Opt-in)	eu-central-2	867642063380

Região da AWS	Código da região	GuardDuty ID da conta de serviço (**`userId`**)
Israel (Tel Aviv) (Opt-in)	il-central-1	619233833001
Europa (Milão) (Opt-in)	eu-south-1	977238331021
Ásia-Pacífico (Hong Kong) (Opt-in)	ap-east-1	249472122084
Oriente Médio (Bahrein) (Opt-in)	me-south-1	404001805210
África (Cidade do Cabo) (Opt-in)	af-south-1	957664736811
Ásia-Pacífico (Jacarta) (Opt-in)	ap-southeast-3	452118225523
Oriente Médio (Emirados Árabes Unidos) (Opt-in)	me-central-1	828603743433
México (Central) Opt-in ()	mx-central-1	557690616787
Ásia-Pacífico (Taipei)	ap-east-2	863518437308
Ásia-Pacífico (Nova Zelândia)	ap-southeast-6	686255982852
AWS GovCloud (US-East)	us-gov-east-1	226283551151
AWS GovCloud (US-West)	us-gov-west-1	226300430612

Cotas na Proteção contra malware para o EC2

Esta seção inclui as cotas associadas ao uso da Proteção contra malware do EC2. Para cotas associadas a GuardDuty, consulteGuardDuty cotas.

A tabela a seguir fornece a disponibilidade padrão de vários recursos quando se usa a Proteção contra malware para o EC2.

Escopo	Padrão	Comentários
Extração e análise de dados em arquivo comprimido ou compactado	5	O número máximo de níveis aninhados permitidos em um arquivo compactado.
Número de arquivos em um arquivo compactado	1000	O número máximo de arquivos que podem ser verificados em um arquivo compactado. Essa contagem é a soma do número de arquivos extraídos do arquivo compactado e do número de arquivos extraídos de todos os arquivos compactados aninhados.
Número de ameaças	32	O número máximo de ameaças que você pode ver no painel de descobert as. GuardDuty O Malware Protection for EC2 pode ter detectado mais nomes de ameaças. Se o número de nomes de ameaças detectado s for maior que o valor padrão, você poderá visualizar os detalhes do JSON seleciona ndo o ID de busca abaixo do nome da descoberta no painel de detalhes do GuardDuty console.
Número de arquivos por ameaça detectada	5	O número máximo de arquivos identificados por ameaça detectada. Por exemplo,

Escopo	Padrão	Comentários
		se GuardDuty detectar 10 arquivos associados a uma única ameaça, a ameaça exibirá no máximo 5 arquivos.
Volumes do EBS por verificação por instância	11	O número máximo de volumes do EBS que GuardDuty podem ser escaneados por instância do EC2. Se houver mais de 11 volumes do EBS que precisam ser verificados, o GuardDuty Malware Protection for EC2 os classifica em `deviceName` ordem alfabética e seleciona os primeiros 11 volumes do EBS.
Tamanho do volume do EBS	2048 GB	Associado a uma instância do Amazon EC2 e a uma carga de trabalho de contêiner, o GuardDuty Malware Protection for EC2 pode escanear cada volume do Amazon EBS com tamanho de até 2048 GB. Essa cota se aplica a cada um Região da AWS em que o suporte à Proteção contra Malware para EC2 está disponível.

Escopo	Padrão	Comentários
Tipos de sistemas de arquivos com suporte	GuardDuty O Malware Protection for EC2 pode verificar os seguintes tipos de sistema de arquivos: • Sistema de arquivos New Technology (NTFS) • Sistema de arquivos X (XFS) • Segundo sistema de arquivos estendido (ext2) • Quarto sistema de arquivos estendido (ext4) • Sistema de arquivos da tabela de alocação de arquivos (FAT) • Sistema de arquivos da tabela de alocação de arquivos virtuais (VFAT)	N/A.
Tags de opções de verificação	50	O número máximo de tags de recursos que podem ser adicionadas para personalizar sua configuração de opções de verificação de malware. Para obter mais informações, consulte Opções de verificação com tags definidas pelo usuário.

Escopo	Padrão	Comentários
Período de retenção da descoberta	90	O número máximo de dias que GuardDuty retém uma descoberta. Para obter as informações mais recentes, consulte GuardDuty Cotas da Amazon.
Período de retenção de verificação de malware	90	O número máximo de dias em que o GuardDuty Malware Protection for EC2 retém o histórico de uma verificação. Para obter mais informaçõ es sobre como visualiza r verificações recentes de malware, consulte Monitoram ento de status e resultados de verificações na Proteção contra Malware para o EC2.
Transações por segundo (TPS) para verificação de On-demand malware	1	O número de solicitações de verificação de On-demand malware que podem ser iniciadas por segundo em cada região.
Limite de intermitência para verificação de On-demand malware	1	O número de solicitações simultâneas de verificação de On-demand malware e malware que podem ser iniciadas por segundo em cada região.

GuardDuty Proteção contra malware para S3

A Proteção contra malware para S3 ajuda você a detectar a presença potencial de malware ao escanear objetos recém-carregados para o bucket do Amazon Simple Storage Service (Amazon S3) que você selecionou. Quando um objeto do S3 ou uma nova versão de um objeto do S3 existente é carregado no bucket selecionado, inicia GuardDuty automaticamente uma verificação de malware.

[Proteção contra malware para o S3 - Visão geral e demonstração]

Duas abordagens para habilitar a Proteção contra malware para o S3

Você pode ativar a Proteção contra Malware para S3 ao ativar o GuardDuty serviço e usar a Proteção contra Malware para S3 como parte da GuardDuty experiência geral, ou quando quiser usar o recurso Proteção contra Malware para S3 sozinho, sem habilitar o serviço. Conta da AWS GuardDuty Quando você ativa a Proteção contra Malware para S3 sozinha, a GuardDuty documentação se refere ao uso da Proteção contra Malware para S3 como um recurso independente.

Considerações sobre o uso independente da Proteção contra malware para S3.

- GuardDuty descobertas de segurança — O Detector ID é um identificador exclusivo associado à sua conta em uma região. Quando você ativa GuardDuty em uma ou mais regiões em uma

conta, uma ID de detector é criada automaticamente para essa conta em cada região em que você ativa GuardDuty. Para obter mais informações, consulte Detector na documentação Conceitos e termos-chave na Amazon GuardDuty.

Quando a Proteção contra malware para o S3 é habilitada de forma independente em uma conta, essa conta não terá um ID de detector associado. Isso afeta quais GuardDuty recursos podem estar disponíveis para você. Por exemplo, quando uma verificação de malware do S3 detecta a presença de malware, nenhuma GuardDuty descoberta será gerada Conta da AWS porque todas as GuardDuty descobertas estão associadas a uma ID de detector.

- Verificar se o objeto escaneado é malicioso — Por padrão, GuardDuty publica os resultados da verificação de malware em seu barramento de EventBridge eventos padrão da Amazon e em um namespace da Amazon CloudWatch . Quando você ativa a marcação no momento da ativação da Proteção contra malware para S3 para um bucket, o objeto S3 escaneado recebe uma tag que menciona o resultado da verificação. Para obter mais informações sobre marcação, consulte Criação opcional de tags de objetos com base no resultado da verificação.

Considerações gerais para habilitar a Proteção contra malware para o S3

As seguintes considerações gerais se aplicam se você usa o Malware Protection for S3 de forma independente ou como parte da GuardDuty experiência:

- Você pode ativar a Proteção contra malware para S3 para um bucket Amazon S3 que pertença à sua própria conta. Como conta de GuardDuty administrador delegado, você não pode habilitar esse recurso em um bucket do Amazon S3 que pertença a uma conta membro.
- Você pode ativar esse recurso nos buckets do S3 que pertencem à mesma região atualmente selecionada no GuardDuty console. GuardDuty não suporta a ativação desse recurso em buckets S3 entre regiões.
- Como conta de GuardDuty administrador delegado, você receberá uma EventBridge notificação da Amazon sempre que houver uma alteração em um bucket Visualizar e entender o status do bucket protegido do S3 que uma das contas membros da sua organização configurou para esse recurso.

Conteúdo

- Preço e custo de uso da Proteção contra Malware para S3
- Como funciona a Proteção contra malware para o S3?
- Capacidades da proteção contra malware para S3

- (Opcional) Comece a usar o GuardDuty Malware Protection for S3 de forma independente (somente console)
- Configurando a proteção contra malware para S3 para seu bucket
- Etapas para habilitar a proteção contra malware para S3
- On-demand Verificação de malware S3 GuardDuty
- Usando controle de acesso baseado em tags (TBAC) com proteção contra malware para S3
- Visualizar e entender o status do bucket protegido
- Monitorando verificações de objetos do S3 na Proteção contra Malware para S3
- Solução de problemas
- Editando o plano de proteção contra malware para um bucket protegido
- Desativando a proteção contra malware para S3 em um bucket protegido
- Suportabilidade dos atributos do Amazon S3
- Quotas na Proteção contra malware para o S3

Preço e custo de uso da Proteção contra Malware para S3

Os preços do Malware Protection for S3 funcionam de forma diferente dos outros planos de proteção do. GuardDuty Enquanto a maioria dos planos de GuardDuty proteção segue um teste gratuito de curto prazo de 30 dias, o Malware Protection for S3 inclui um nível gratuito. AWS Para obter informações sobre GuardDuty preços, consulte Preços em GuardDuty.

A lista a seguir fornece os custos de preços associados ao uso da Proteção contra Malware para S3.

Nível gratuito (custo de digitalização)

Cada um Conta da AWS recebe um nível gratuito que inclui o uso de até um limite específico por mês para cada região. Cada um Conta da AWS recebe um nível gratuito mensal de uso de até 1.000 solicitações e 1 GB de dados digitalizados. Se seu uso ultrapassar o limite especificado, você começará a incorrer no custo de uso do limite excedido. Para obter detalhes completos sobre preços, consulte os preços GuardDuty dos planos de proteção.

> **Important**
>
> On-demand a digitalização não está incluída no nível gratuito.

Para obter informações sobre o custo de uso após a ativação da Proteção contra Malware para S3, consulteAnalisando o custo de uso da Proteção contra Malware para S3.

Custo de uso da marcação de objetos do S3

Quando você ativa a Proteção contra Malware para S3, é opcional habilitar a marcação para seus objetos verificados do S3. Quando você opta por ativar a marcação de objetos do S3, há um custo de uso associado. Para obter mais informações sobre os custos, consulte guia Gerenciamento e insights na página de preços do Amazon S3.

O custo de uso da marcação de objetos do S3 não está incluído no nível gratuito.

APIs do Amazon S3 — GET e custo de uso PUT

Você incorrerá em custos de uso ao GuardDuty executar as APIs do Amazon S3 com base na função do IAM. Por exemplo, depois de assumir a função do IAM, GuardDuty executa a `PutObject` API para adicionar o objeto de teste ao bucket selecionado. Isso ajuda a GuardDuty avaliar o status ativado do recurso.

Para obter informações sobre preços de chamadas de API do S3 em seu Região da AWS, consulte Solicitações e recuperação de dados na guia Armazenamento e solicitações na página de preços do Amazon S3.

O custo de uso das APIs do Amazon S3 não está incluído no nível gratuito.

EventBridge Custo da regra gerenciada

GuardDuty usa uma regra EventBridge gerenciada para detectar quando novos objetos são carregados em seus buckets protegidos. Você incorrerá em custos para os eventos opcionais do Amazon S3 ingeridos por. EventBridge Você não incorrerá em custos de entrega do evento. Para obter mais informações sobre definição de preço do EventBridge, consulte Definição de preço do EventBridge .

EventBridge O custo da regra gerenciada não está incluído no nível gratuito.

Analisando o custo de uso da Proteção contra Malware para S3

Sua conta começa a incorrer em custos de uso quando você usa o Malware Protection for S3 além do limite específico do nível gratuito. Para obter informações sobre o nível gratuito, consultePreço e custo de uso da Proteção contra Malware para S3. Observe que o nível gratuito não se aplica à proteção contra malware para escaneamento de objetos sob demanda do S3.

O GuardDuty console não suporta a revisão do custo de uso do Malware Protection for S3. Para ver o custo de uso, navegue até Cost Explorer no https://console.aws.amazon.com/costmanagement/console. Para obter informações sobre Conta da AWS faturamento, consulte o Guia do AWS Billing usuário.

Para obter informações sobre o custo estimado de uso em GuardDuty, consulteMonitorando o uso e estimando custos.

Como funciona a Proteção contra malware para o S3?

Esta seção descreve os componentes da Proteção contra malware para o S3, como ela funciona depois de habilitada para um bucket do S3 e como é possível revisar o status e o resultado da verificação de malware.

Visão geral do

Você pode ativar o Malware Protection for S3 para um bucket Amazon S3 que pertença ao seu. Conta da AWS GuardDutyoferece flexibilidade para ativar esse recurso para todo o bucket ou limitar o escopo da verificação de malware a prefixos de objetos específicos, onde GuardDuty verifica o conteúdo de cada objeto carregado que começa com um dos prefixos selecionados. É possível adicionar até 5 prefixos. Ao ativar o recurso para um bucket S3, esse bucket é chamado de bucket protegido.

Permissões de perfil do IAM

O Malware Protection for S3 usa uma função do IAM que permite GuardDuty realizar as ações de verificação de malware em seu nome. Entre essas ações estão ser notificado sobre os objetos recém-carregados no bucket selecionado, ler esses objetos e, opcionalmente, adicionar tags aos objetos lidos. Trata-se de um pré-requisito para configurar seu bucket S3 com esse recurso.

Existe a opção de atualizar uma função do IAM existente ou criar uma nova função para essa finalidade. Ao habilitar a Proteção contra malware para o S3 para mais de um bucket, é possível atualizar a função do IAM existente para incluir o nome do outro bucket, caso necessário. Para obter mais informações, consulte Criar ou atualizar a política do perfil do IAM.

Criação opcional de tags de objetos com base no resultado da verificação

Ao habilitar a Proteção contra malware para o S3 para o seu bucket, há uma etapa opcional para habilitar a criação de tags para objetos S3 lidos. A função do IAM já inclui a permissão para adicionar

tags ao seu objeto após a verificação. No entanto, GuardDuty adicionará tags somente quando você ativar essa opção no momento da configuração.

Deve-se habilitar essa opção antes que um objeto seja carregado. Depois que a varredura terminar, GuardDuty adiciona uma tag predefinida ao objeto S3 digitalizado com o seguinte par chave/valor:

`GuardDutyMalwareScanStatus:`*`Potential scan result`*

Os possíveis valores da tag de resultado da verificação incluem `NO_THREATS_FOUND`, `THREATS_FOUND`, `UNSUPPORTED`, `ACCESS_DENIED` e `FAILED`. Para obter mais informações sobre esses valores, consulte the section called “Status de verificação potencial do objeto S3 e status do resultado”.

A habilitação da criação de tags é uma das maneiras de saber sobre o resultado da verificação do objeto S3. Além disso, é possível usar essas tags para adicionar uma política de recursos do S3 de controle de acesso baseado em tags (TBAC), para que seja possível tomar medidas em relação aos objetos possivelmente maliciosos. Para obter mais informações, consulte Adicionando TBAC ao recurso do bucket do S3.

Recomendamos que a habilitação da colocação de tags seja feita no momento da configuração da Proteção contra malware para o S3 para o seu bucket. Se você ativar a marcação após o upload de um objeto e, potencialmente, o escaneamento iniciar, não GuardDuty será possível adicionar tags ao objeto digitalizado. Para obter informações sobre o custo associado com a colocação de tags em objetos S3, consulte Preço e custo de uso da Proteção contra Malware para S3.

Processe depois de habilitar a Proteção contra malware para o S3 para um bucket

Depois de habilitar a Proteção contra malware para o S3, um recurso do plano de Proteção contra Malware é criado exclusivamente para o bucket do S3 selecionado. Esse recurso está associado a um ID do plano de Proteção contra malware, um identificador exclusivo para seu recurso protegido. Ao usar uma das permissões do IAM GuardDuty , cria e gerencia uma regra EventBridge gerenciada com o nome de`DO-NOT-DELETE-AmazonGuardDutyMalwareProtectionS3*`.

Como GuardDuty lida com seus dados - proteções para proteção de dados

O Malware Protection for S3 escuta as notificações da Amazon EventBridge . Quando um objeto é carregado no bucket selecionado ou em um dos prefixos, GuardDuty baixa esse objeto do bucket do S3 usando um AWS PrivateLinke depois o lê, descriptografa e digitaliza em um ambiente isolado na mesma região. O ambiente de verificação é executado em uma nuvem privada virtual (VPC)

bloqueada, sem acesso à Internet. A VPC está conectada a um grupo de regras de firewall de DNS que permite a comunicação somente com os domínios listados como permitidos que são proprietários. AWS Durante o escaneamento, armazena GuardDuty temporariamente o objeto S3 baixado no ambiente de escaneamento que é criptografado com as chaves AWS Key Management Service (AWS KMS).

> **Note**
>
> Por padrão, todas as APIs do Amazon S3 listadas sob o tipo de evento Objeto criado no Guia do usuário do Amazon S3 iniciarão a verificação da Proteção contra malware para o S3. Esses tipos de eventos incluem PutObjectPOST Object CompleteMultipartUploade. CopyObject

Para obter informações sobre a metodologia de detecção de GuardDuty malware e os mecanismos de verificação que ela usa, consulteGuardDuty mecanismo de verificação de detecção de malware.

Após a conclusão da verificação de malware, GuardDuty processa os metadados da verificação com o status da verificação e, em seguida, exclui a cópia baixada do objeto.

GuardDuty limpa o ambiente de escaneamento toda vez antes do início de um novo escaneamento. GuardDuty usa autorização contingente para o acesso do operador ao ambiente de digitalização, e cada solicitação de acesso é analisada, aprovada e auditada.

Analisando o status e o resultado da verificação de objetos do S3

GuardDuty publica o evento de resultado da digitalização de objetos do S3 no barramento de eventos EventBridge padrão da Amazon. GuardDuty também envia as métricas de escaneamento, como número de objetos escaneados e bytes escaneados, para a Amazon. CloudWatch Se você ativou a marcação, GuardDuty adicionará a tag predefinida `GuardDutyMalwareScanStatus` e um possível resultado de escaneamento como o valor da tag.

> **Important**
>
> GuardDuty usa entrega pelo menos uma vez, o que significa que você pode receber vários resultados de escaneamento para o mesmo objeto. Recomendamos projetar suas aplicações para lidar com resultados duplicados. Você é cobrado apenas uma vez por cada objeto verificado.

Para obter mais informações, consulte Monitorando verificações de objetos do S3 na Proteção contra Malware para S3.

Revisar descobertas geradas

A análise das descobertas depende se você está ou não usando o Malware Protection for S3 com. GuardDuty Considere os seguintes cenários:

Usando a Proteção contra Malware para S3 quando o GuardDuty serviço está ativado (ID do detector)

- Se a verificação de malware detectar um arquivo potencialmente malicioso em um objeto do S3, GuardDuty gerará uma descoberta associada. É possível visualizar os detalhes da descoberta e usar as etapas recomendadas para corrigir a descoberta. Com base na frequência de suas descobertas de exportação, a descoberta gerada é exportada para um bucket do S3 e um barramento de EventBridge eventos.

  Para obter informações sobre o tipo de descoberta que seria gerado, consulteTipo de descoberta da Proteção contra malware para S3.

Como usar a Proteção contra malware para o S3 como um recurso independente (sem ID de detector)

- GuardDuty não será capaz de gerar descobertas porque não há uma ID de detector associada. Para saber o status da verificação de malware do objeto S3, você pode visualizar o resultado da verificação que é publicado GuardDuty automaticamente no seu barramento de eventos padrão. Você também pode visualizar as CloudWatch métricas para avaliar o número de objetos e bytes que GuardDuty tentaram escanear. Você pode configurar CloudWatch alarmes para ser notificado sobre os resultados da verificação. Caso tenha habilitado a colocação de tags em objetos S3, também é possível visualizar o status da verificação de malware verificando no objeto S3 a chave da tag e o `GuardDutyMalwareScanStatus` valor da tag do resultado da verificação.

  Para obter informações sobre o status e o resultado da verificação de objetos S3, consulte Monitorando verificações de objetos do S3 na Proteção contra Malware para S3.

Capacidades da proteção contra malware para S3

A lista a seguir fornece uma visão geral do que você pode esperar ou fazer depois de ativar a Proteção contra Malware para S3 em seu bucket:

- Escolha o que verificar — Examine os arquivos à medida que eles são carregados em todos os prefixos ou em prefixos específicos (até 5) associados ao bucket do S3 selecionado.
- Escaneamentos automáticos em objetos enviados — Depois de ativar o Malware Protection for S3 para um bucket, GuardDuty iniciará automaticamente um escaneamento para detectar possíveis malwares em um objeto recém-carregado.
- On-demand escaneamentos — Você pode iniciar escaneamentos de objetos existentes ou digitalizar novamente objetos digitalizados anteriormente. Para obter mais informações, consulte On-demand Verificação de malware S3 GuardDuty.
- Ativar por meio do console, usando API/AWS CLI, ou CloudFormation — Escolha um método preferido para ativar a Proteção contra Malware para S3.

  Você pode ativar a Proteção contra Malware para S3 usando plataformas de infraestrutura como código (IaC), como o Terraform. Para mais informações, consulte Recurso: `aws_guardduty_malware_protection_plan`.
- Formatos de arquivo compatíveis, cotas de Proteção contra Malware para S3 e atributos do Amazon S3 – a Proteção contra Malware para S3 oferece suporte a todos os formatos de arquivo que você pode carregar nos buckets do S3. Se o arquivo enviado estiver protegido por senha e GuardDuty for capaz de detectar a presença de proteção por senha para o tipo do arquivo enviado, GuardDuty tentará escanear o conteúdo original usando senhas comuns. Se a senha falhar, a verificação será ignorada. GuardDuty não consigo detectar a presença de proteção por senha em todos os formatos de arquivo. Se não GuardDuty conseguir detectar a presença de proteção por senha, ele ainda GuardDuty digitalizará o conteúdo criptografado.

  Para obter informações sobre as cotas relacionadas ao tamanho do objeto, nível máximo de profundidade de arquivamento e outros detalhes, consulteQuotas na Proteção contra malware para o S3.

  Para obter informações sobre se um atributo do Amazon S3 é suportado ou não, consulte. Suportabilidade dos atributos do Amazon S3
- Suporta a marcação de objetos S3 escaneados — Quando você ativaCriação opcional de tags de objetos com base no resultado da verificação, depois de cada verificação de malware, GuardDuty adiciona uma tag que indica o status da verificação. É possível usar essa tag para configurar o controle de acesso baseado em tags (TBAC) para os objetos do S3. Por exemplo, você pode restringir o acesso aos objetos do S3 indicados como maliciosos e ter o valor da tag como`THREATS_FOUND`.

- EventBridge Notificações da Amazon — GuardDuty envia eventos para a Amazon EventBridge quando o status do recurso do plano de Proteção contra Malware muda ou quando uma verificação de malware do objeto S3 é concluída. Os eventos são enviados para o barramento de eventos padrão. Você pode usar EventBridge esses eventos para escrever regras que executam ações, como monitorar quando esses eventos acontecem. Para obter mais informações, consulte Monitoramento de escaneamentos de objetos do S3 com a Amazon EventBridge.
- CloudWatch métricas — Visualize CloudWatch métricas para ativar alarmes sobre determinados status de escaneamento de malware. Para obter mais informações, consulte Métricas de status de escaneamento de objetos do S3 em CloudWatch.

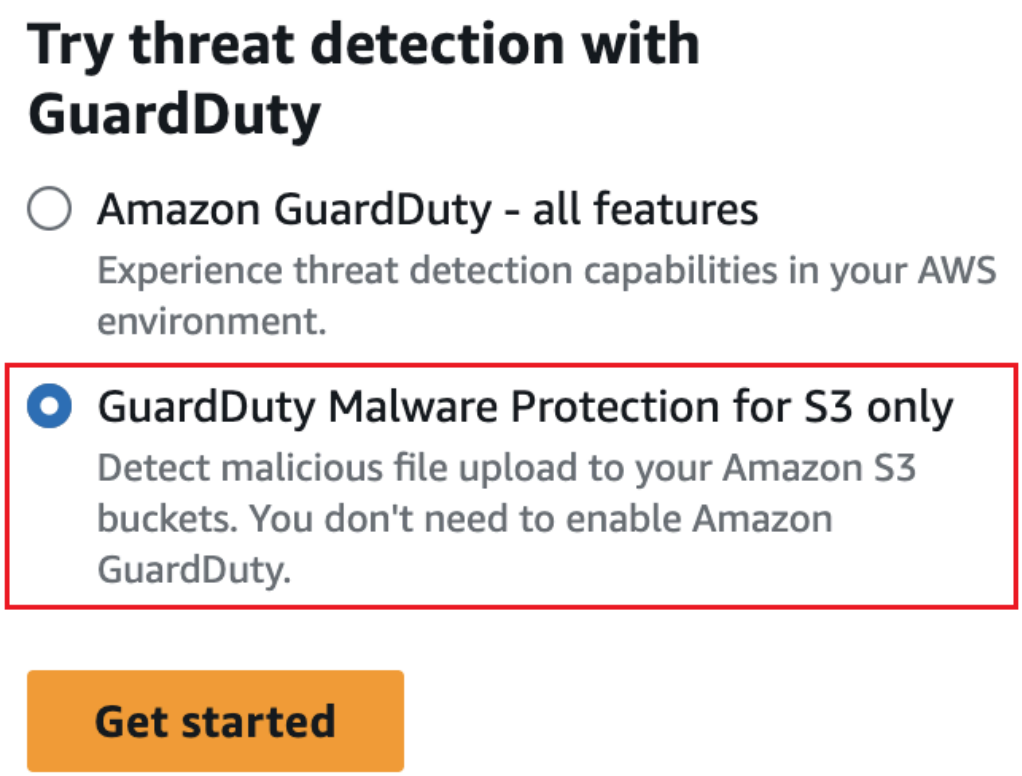
(Opcional) Comece a usar o GuardDuty Malware Protection for S3 de forma independente (somente console)

Use essa etapa opcional quando quiser começar a usar a opção de detecção de ameaças do Malware Protection for S3, independentemente do GuardDuty status em seu Conta da AWS.

Se você também quiser usar outros planos de proteção dedicados GuardDuty, você deve começar a usar o GuardDuty serviço da Amazon. Para obter informações sobre planos de GuardDuty proteção, consulteCaracterísticas do GuardDuty. Quando você já tiver ativado GuardDuty sua conta, poderá pular esta etapa e continuar. Configurando a proteção contra malware para S3 para seu bucket

Etapas para começar a usar a Proteção contra Malware para S3 somente para detecção de ameaças

1. Faça login no Console de gerenciamento da AWS e abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.
2. Selecione Proteção contra GuardDuty malware somente para S3. Isso ajuda você a detectar se um arquivo recém-carregado no bucket do Amazon Simple Storage Service (Amazon S3) potencialmente contém malware.



3. Escolha Começar. Agora você pode continuar com as etapas abaixo Configurando a proteção contra malware para S3 para seu bucket.

Configurando a proteção contra malware para S3 para seu bucket

Para que a Proteção contra Malware para S3 verifique e (opcionalmente) adicione tags aos seus objetos do S3, você pode usar funções de serviço que tenham as permissões necessárias para realizar ações de verificação de malware em seu nome. Para obter mais informações sobre o uso de perfis de serviço para habilitar a proteção contra malware para o S3, consulte Service Access. Essa função é diferente da função vinculada ao serviço de Proteção contra GuardDuty Malware.

Se preferir usar funções do IAM, você pode anexar uma função do IAM que inclua as permissões necessárias para digitalizar e (opcionalmente) adicionar tags aos seus objetos do S3. GuardDuty em seguida, assume essa função do IAM para realizar essas ações em seu nome. Você precisará desse nome de perfil do IAM no momento de habilitar esse plano de proteção para seu bucket do Amazon S3.

Se você estiver usando perfil do IAM, para toda vez que quiser proteger um bucket do Amazon S3, você deve executar as duas etapas listadas nesta seção.

Para ativar a proteção contra malware para o S3, você precisará de detalhes como o nome do bucket do S3, prefixos de objeto, se quiser focar a proteção em prefixos específicos, e o nome do perfil do IAM com as permissões necessárias.

As etapas permanecem as mesmas, independentemente de você começar a usar o Malware Protection for S3 de forma independente ou habilitá-lo como parte do GuardDuty serviço.

Tópicos

1. Criar ou atualizar a política do perfil do IAM
2. Habilitando a proteção contra malware para S3 para seu bucket
3. Solução de problemas de erro de permissões de perfil do IAM

Habilitando a proteção contra malware para S3 para seu bucket

Esta seção fornece etapas detalhadas sobre como habilitar a Proteção contra Malware para S3 para um bucket em sua própria conta. Antes de continuar, analise as seguintes considerações:

- Quando você ativa esse plano de proteção usando o GuardDuty console, ele inclui a etapa para criar uma nova função ou usar uma função existente na seção Acesso ao serviço.
- Ao habilitar esse plano de proteção usando a GuardDuty API ou a CLI, é necessário Criar ou atualizar a política do perfil do IAM antes de continuar.
- Independentemente de como você habilitar esse plano de proteção, você deve ter as Permissões para criar um recurso do plano de Proteção contra malware necessárias.

Considerando o controle de utilização do bucket do Amazon S3

O controle de utilização do S3 pode limitar a taxa na qual os dados podem ser transferidos de ou para seus buckets do Amazon S3. Isso pode potencialmente atrasar as verificações de malware de seus objetos recém-carregados.

Se você espera grandes volumes de solicitações `GET` e `PUT` para seus buckets do S3, considere implementar medidas para evitar o controle de utilização. Para obter informações sobre como fazer isso, consulte Prevenir o controle de utilização do Amazon S3 no Guia do usuário do Amazon Athena.

Permissões para criar um recurso do plano de Proteção contra malware

Quando você ativa a proteção contra malware para S3 para um bucket do Amazon S3, GuardDuty cria um recurso do plano de proteção contra malware que atua como um identificador para o plano de proteção do bucket. Se você ainda não estiver usando a AWS política gerenciada: AmazonGuardDutyFullAccess_v2 (recomendado), adicione as seguintes permissões para criar esse recurso:

- `guardDuty:CreateMalwareProtectionPlan`
- `iam:PassRole`

Você pode usar o exemplo de política personalizada a *`placeholder values`* seguir e substituí-lo pelos valores apropriados para sua conta:

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "iam:PassRole"
            ],
            "Resource": "arn:aws:iam::111122223333:role/role-name",
            "Condition": {
                "StringEquals": {
                    "iam:PassedToService": "malware-protection-
plan.guardduty.amazonaws.com"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "guardduty:CreateMalwareProtectionPlan"
            ],
            "Resource": "*"
        }
    ]
```

```
}
```

Ativando a proteção contra malware para o S3 usando o console GuardDuty

As seções a seguir fornecem um passo a passo, como você experimentará no console. GuardDuty

Para ativar a proteção contra malware para o S3 usando o console GuardDuty

Entre nos detalhes do bucket do S3

Use as etapas a seguir para fornecer detalhes do bucket do Amazon S3:

1. Faça login no Console de gerenciamento da AWS e abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.
2. Usando o Região da AWS seletor no canto superior direito da página, selecione a região em que você deseja ativar a proteção contra malware para o S3.
3. No painel de navegação, escolha Proteção contra Malware para S3
4. Na seção Buckets protegidos, escolha Habilitar para ativar a Proteção contra Malware para S3 para um bucket S3 que pertence ao seu Conta da AWS.
5. Em Inserir detalhes do bucket do S3, insira o nome do Bucket do Amazon S3. Como alternativa, escolha Browse S3 para selecionar um bucket S3.

   O Região da AWS do bucket do S3 e o Conta da AWS local em que você habilita a proteção contra malware para o S3 devem ser os mesmos. Por exemplo, se sua conta pertence à região `us-east-1`, a região do bucket do Amazon S3 também deve ser `us-east-1`.
6. Em Prefixo, você pode selecionar Todos os objetos no bucket do S3 ou Objetos que começam com um prefixo específico.

   - Selecione Todos os objetos no bucket do S3 quando quiser GuardDuty escanear todos os objetos recém-carregados no bucket selecionado.
   - Selecione Objetos que começam com um prefixo específico quando quiser verificar os objetos recém-carregados que pertencem a um prefixo específico. Essa opção ajuda você a focar no escopo da verificação de malware somente nos prefixos de objeto selecionados. Para obter informações sobre como usar pastas no Amazon S3, consulte Organizar objetos no console do Amazon S3 usando pastas no Manual do usuário do Amazon S3.

     Escolha Adicionar prefixo e insira o prefixo. Você pode adicionar até cinco prefixos.

Ativar marcação para objetos verificados

Esta é uma etapa opcional. Quando você ativa a opção de marcação antes de um objeto ser carregado em seu bucket, depois de concluir a verificação, GuardDuty adiciona uma tag predefinida com a chave como `GuardDutyMalwareScanStatus` e o valor como resultado da verificação. Para usar a Proteção contra Malware para S3 de forma otimizada, recomendamos ativar a opção de adicionar uma tag aos objetos do S3 após o término da verificação. O custo padrão da atribuição de tags de objetos do S3 é aplicável. Para obter mais informações, consulte Preço e custo de uso da Proteção contra Malware para S3.

Por que você deve ativar a marcação?

- Ativar a marcação é uma das maneiras de saber sobre o resultado da verificação de malware. Para obter informações sobre o resultado de uma verificação de malware do S3, consulte Monitorando verificações de objetos do S3 na Proteção contra Malware para S3.
- Configure uma política de controle de acesso baseado em tags (TBAC) em seu bucket do S3 que contém o objeto potencialmente malicioso. Para obter informações sobre como implementar um controle de acesso baseado em tags (TBAC), consulte. Usando controle de acesso baseado em tags (TBAC) com proteção contra malware para S3

Considerações GuardDuty para adicionar uma tag ao seu objeto do S3:

- Por padrão. você pode associar até 10 tags a um objeto. Para obter informações, consulte Categorizando o armazenamento usando tags no Guia do usuário do Amazon S3.

  Se todas as 10 tags já estiverem em uso, não é GuardDuty possível adicionar a tag predefinida ao objeto digitalizado. GuardDuty também publica o resultado da verificação em seu barramento de EventBridge eventos padrão. Para obter mais informações, consulte Monitoramento de escaneamentos de objetos do S3 com a Amazon EventBridge.
- Quando a função do IAM selecionada não inclui a permissão GuardDuty para marcar o objeto S3, mesmo com a marcação ativada para seu bucket protegido, não GuardDuty será possível adicionar uma tag a esse objeto S3 digitalizado. Para obter mais informações sobre como criar uma permissão do perfil do IAM para marcação de tag, consulte Criar ou atualizar a política do perfil do IAM.

  GuardDuty também publica o resultado da verificação em seu barramento de EventBridge eventos padrão. Para obter mais informações, consulte Monitoramento de escaneamentos de objetos do S3 com a Amazon EventBridge.

Para selecionar uma opção em Marcar objetos verificados

- Quando quiser adicionar tags GuardDuty aos objetos escaneados do S3, selecione Marcar objetos.
- Quando você não quiser adicionar tags GuardDuty aos objetos escaneados do S3, selecione Não marcar objetos.

Acesso ao serviço

Use as etapas a seguir para escolher um perfil de serviço existente ou criar um novo perfil de serviço que tenha as permissões necessárias para executar ações de verificação de malware em seu nome. Essas ações podem incluir a verificação dos objetos S3 recém-carregados e (opcionalmente) a adição de tags a esses objetos. Para mais informações sobre as permissões que esse perfil terá, consulte Criar ou atualizar a política do perfil do IAM.

Na seção Acesso ao serviço selecione uma das seguintes opções:

1. Criar e usar um novo perfil de serviço — Você pode criar e usar um novo perfil de serviço que tenha as permissões necessárias para realizar a verificação de malware.

   Em Nome da função, você pode escolher usar o nome pré-preenchido por GuardDuty ou inserir um nome significativo de sua escolha para identificar a função. Por exemplo, `GuardDutyS3MalwareScanRole`. O nome do perfil deve ter de 1 a 64 caracteres. Os caracteres válidos são a-z A-Z, 0-9 e '+=, .@-_'.
2. Usar um perfil de serviço existente — Você pode escolher um perfil de serviço existente na lista de Nome do perfil de serviço.

   a. Em Modelo de política, você pode visualizar a política do seu bucket do S3. Verifique se você inseriu ou selecionou um bucket do S3 na seção de detalhes Inserir bucket do S3.

   b. Em Nome do perfil de serviço, escolha um perfil de serviço na lista de perfis de serviço.

Você pode fazer alterações na política com base em seus requisitos. Para obter mais detalhes sobre como criar ou atualizar um perfil do IAM, consulte Criar ou atualizar a política de perfil do IAM.

Para problemas com as permissões de perfil do IAM, consulte Solução de problemas de erro de permissões de perfil do IAM.

(Opcional) Etiquetar ID do plano de proteção contra malware

Essa é uma etapa opcional que ajuda você a adicionar tags ao recurso do plano de proteção contra malware que seriam criadas para seu recurso de bucket do S3.

Cada tag tem duas partes: uma chave de tag e um valor de tag opcional. Para obter mais informações sobre marcação e seus benefícios, consulte Recursos de marcação AWS .

Para adicionar tags ao seu recurso de plano de proteção contra malware

1. Digite uma chave e, opcionalmente, um valor para a tag. A chave e o valor da tag diferenciam maiúsculas de minúsculas. Para obter informações sobre os nomes da chave e do valor da tag, consulte Limites e requisitos de nomenclatura da tag.
2. Para adicionar mais tags ao seu recurso do plano de Proteção contra Malware, escolha Adicionar nova tag e repita a etapa anterior. Você pode adicionar até 50 tags a cada recurso.
3. Escolha Habilitar.

Ativando a proteção contra malware para o S3 usando API/CLI

Esta seção inclui as etapas para quando você quiser ativar a Proteção contra malware para S3 de forma programática em seu ambiente. AWS Isso requer o nome do recurso da Amazon (ARN) do perfil do IAM que você criou nesta etapa - Criar ou atualizar a política do perfil do IAM.

Para ativar a proteção contra malware para o S3 de forma programática usando API/CLI

- Usando a API

  Execute o CreateMalwareProtectionPlan para ativar a Proteção contra malware para S3 em um bucket que pertence à sua própria conta.
- Usando AWS CLI

  Dependendo de como você deseja ativar a Proteção contra malware para o S3, a lista a seguir fornece AWS CLI exemplos de comandos para casos de uso específicos. Ao executar esses comandos, substitua o*`placeholder examples shown in red`*, pelos valores apropriados para sua conta.

  AWS CLI comandos de exemplo

  - Use o AWS CLI comando a seguir para ativar a Proteção contra malware para S3 em um bucket sem marcação para objetos do S3 escaneados:

```
aws guardduty create-malware-protection-plan --role
 "arn:aws:iam::111122223333:role/role-name" --protected-resource
 "S3Bucket"={"BucketName"="amzn-s3-demo-bucket1"}
```

- Use o AWS CLI comando a seguir para ativar a Proteção contra malware do S3 para um bucket com prefixos de objeto específicos e sem marcação para objetos do S3 escaneados:

```
aws guardduty create-malware-protection-plan --role
 "arn:aws:iam::111122223333:role/role-name" --protected-resource '{"S3Bucket":
{"BucketName":"amzn-s3-demo-bucket1", "ObjectPrefixes": ["Object1","Object1"]}}'
```

- Use o AWS CLI comando a seguir para ativar a proteção contra malware do S3 para um bucket com a marcação de objetos do S3 digitalizados ativada:

```
aws guardduty create-malware-protection-plan --role
 "arn:aws:iam::111122223333:role/role-name" --protected-resource
 "S3Bucket"={"BucketName"="amzn-s3-demo-bucket1"} --actions
 "Tagging"={"Status"="ENABLED"}
```

Depois de executar esses comandos com êxito, um ID exclusivo do plano de Proteção contra Malware será gerado. Para realizar ações como atualizar ou desativar o plano de proteção do seu bucket, você precisará desse ID do plano de proteção contra malware.

Para problemas com as permissões de perfil do IAM, consulte Solução de problemas de erro de permissões de perfil do IAM.

Criar ou atualizar a política do perfil do IAM

Para que a Proteção contra Malware Protection para S3 verifique e (opcionalmente) adicione tags aos seus objetos do S3, você pode usar perfis de serviço que tenham as permissões necessárias para realizar ações de verificação de malware em seu nome. Para obter mais informações sobre o uso de perfis de serviço para habilitar a proteção contra malware para o S3, consulte Service Access. Essa função é diferente da função vinculada ao serviço de Proteção contra GuardDuty Malware.

Se você preferir usar perfis do IAM, pode anexar um perfil do IAM que inclua as permissões necessárias para verificar e (opcionalmente) adicionar tags aos seus objetos do S3. Você deve criar um perfil do IAM ou atualizar o perfil existente para incluir essas permissões. Como essas permissões são necessárias para cada bucket do Amazon S3 para o qual você habilita a proteção

contra malware para o S3, você precisa executar essa etapa para cada bucket do Amazon S3 que você deve proteger.

A lista a seguir explica como determinadas permissões ajudam a GuardDuty realizar a verificação de malware em seu nome:

- Permita que EventBridge as ações da Amazon criem e gerenciem a regra EventBridge gerenciada para que o Malware Protection for S3 possa ouvir suas notificações de objetos do S3.

  Para obter mais informações, consulte as regras EventBridge gerenciadas pela Amazon no Guia EventBridge do usuário da Amazon.
- Permita que o Amazon S3 e EventBridge as ações enviem notificações EventBridge para todos os eventos neste bucket

  Para obter mais informações, consulte Habilitando a Amazon EventBridge no Guia do usuário do Amazon S3.
- Permita que as ações do Amazon S3 acessem o objeto S3 carregado e adicionem uma tag predefinida,`GuardDutyMalwareScanStatus`, ao objeto S3 verificado. Ao usar um prefixo de objeto, adicione uma condição `s3:prefix` somente nos prefixos de destino. Isso GuardDuty impede o acesso a todos os objetos do S3 em seu bucket.
- Permita que as principais ações do KMS acessem o objeto antes de digitalizar e colocar um objeto de teste em buckets com o suporte DSSE-KMS e SSE-KMS a criptografia.

> **Note**
>
> Essa etapa é necessária sempre que você ativa a Proteção de Malware para S3 em um bucket na sua conta. Se você já tem um perfil do IAM, pode atualizar sua política para incluir os detalhes de outro recurso do bucket do Amazon S3. O tópico Adicionar permissões de política do IAM fornece um exemplo de como fazer isso.

Use as etapas a seguir para criar ou atualizar uma política e um perfil do IAM.

Políticas

- Adicionar permissões de política do IAM
- Adicionar Política de relação de confiança

Adicionar permissões de política do IAM

Você pode optar por atualizar a política em linha de um perfil do IAM existente ou criar um novo perfil do IAM. Para obter mais informações sobre as etapas, consulte Criar perfis do IAM, ou Modificar uma política de permissões de perfil no Guia do usuário do IAM.

Adicione o seguinte modelo de permissões ao seu perfil do IAM preferido. Substitua os seguintes valores de espaço reservado por valores apropriados associados à sua conta:

- Para*amzn-s3-demo-bucket*, substitua pelo nome do seu bucket do Amazon S3.

  Para usar o mesmo perfil do IAM para mais de um recurso de bucket do S3, atualize uma política existente conforme exibido no exemplo a seguir:

  ```
  ...
  ...
  "Resource": [
      "arn:aws:s3:::amzn-s3-demo-bucket/*",
      "arn:aws:s3:::amzn-s3-demo-bucket2/*"
  ],
  ...
  ...
  ```

  Certifique-se de adicionar uma vírgula (,) antes de adicionar um novo ARN associado ao bucket do S3. Faça isso sempre que você se referir a um bucket do S3 `Resource` no modelo de política.
- Para*111122223333*, substitua pelo seu Conta da AWS ID.
- Para*us-east-1*, substitua pelo seu Região da AWS.
- Para *APKAEIBAERJR2EXAMPLE*, substitua pelo ID da chave gerenciada pelo cliente. Se seu bucket do S3 for criptografado usando uma AWS KMS chave, adicionaremos as permissões relevantes se você escolher a opção Criar uma nova função ao configurar a proteção contra malware para seu bucket.

  ```
  "Resource": "arn:aws:kms:us-east-1:111122223333:key/*"
  ```

Modelo de política de perfil do IAM

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [{
            "Sid": "AllowManagedRuleToSendS3EventsToGuardDuty",
            "Effect": "Allow",
            "Action": [
                "events:PutRule",
                "events:DeleteRule",
                "events:PutTargets",
                "events:RemoveTargets"
            ],
            "Resource": [
                "arn:aws:events:us-east-1:111122223333:rule/DO-NOT-DELETE-
AmazonGuardDutyMalwareProtectionS3*"
            ],
            "Condition": {
                "StringLike": {
                    "events:ManagedBy": "malware-protection-
plan.guardduty.amazonaws.com"
                }
            }
        },
        {
            "Sid": "AllowGuardDutyToMonitorEventBridgeManagedRule",
            "Effect": "Allow",
            "Action": [
                "events:DescribeRule",
                "events:ListTargetsByRule"
            ],
            "Resource": [
                "arn:aws:events:us-east-1:111122223333:rule/DO-NOT-DELETE-
AmazonGuardDutyMalwareProtectionS3*"
            ]
        },
        {
            "Sid": "AllowPostScanTag",
            "Effect": "Allow",
            "Action": [
                "s3:PutObjectTagging",
                "s3:GetObjectTagging",
                "s3:PutObjectVersionTagging",
```

```
                "s3:GetObjectVersionTagging"
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-bucket/*"
            ]
        },
        {
            "Sid": "AllowEnableS3EventBridgeEvents",
            "Effect": "Allow",
            "Action": [
                "s3:PutBucketNotification",
                "s3:GetBucketNotification"
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-bucket"
            ]
        },
        {
            "Sid": "AllowPutValidationObject",
            "Effect": "Allow",
            "Action": [
                "s3:PutObject"
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-bucket/malware-protection-resource-
validation-object"
            ]
        },
        {
            "Sid": "AllowCheckBucketOwnership",
            "Effect": "Allow",
            "Action": [
                "s3:ListBucket"
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-bucket"
            ]
        },
        {
           "Sid": "AllowMalwareScan",
            "Effect": "Allow",
            "Action": [
                "s3:GetObject",
                "s3:GetObjectVersion"
```

```
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-bucket/*"
            ]
        },
        {
            "Sid": "AllowDecryptForMalwareScan",
            "Effect": "Allow",
            "Action": [
                "kms:GenerateDataKey",
                "kms:Decrypt"
            ],
            "Resource": "arn:aws:kms:us-
east-1:111122223333:key/APKAEIBAERJR2EXAMPLE",
            "Condition": {
                "StringLike": {
                    "kms:ViaService": "s3.us-east-1.amazonaws.com"
                }
            }
        }
    ]
}
```

Adicionar Política de relação de confiança

Anexe a política a seguir ao seu perfil do IAM: Para obter mais informações, consulte Modificar uma política de confiança de perfil (console).

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "malware-protection-plan.guardduty.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
```

```
}
```

Solução de problemas de erro de permissões de perfil do IAM

Ao ativar a Proteção contra malware para o S3, GuardDuty verifique se sua função de serviço do IAM tem as permissões necessárias para validar a propriedade do bucket do Amazon S3. Se essas permissões estiverem ausentes ou configuradas incorretamente, você poderá receber a seguinte mensagem:

```
"message": "The request was rejected because provided IAM role does not have the
 required permissions to validate S3 bucket ownership."
"type": "InvalidInputException"
```

Os cenários a seguir podem ajudar a solucionar esse erro:

Permissões de função do IAM ausentes

- O perfil do IAM deve ter as permissões necessárias para permitir que a Proteção contra Malware para S3 assuma esse perfil.
- GuardDuty valida a propriedade do bucket com a `"s3:ListBucket"` permissão. Isso deve estar presente no perfil do IAM que você usa.

  Para obter mais informações sobre as permissões, consulte Criar ou atualizar a política do perfil do IAM.

Disponibilidade do perfil do IAM

- Ao criar um novo perfil do IAM, aguarde alguns minutos para que as alterações atinjam a consistência final antes de habilitar a Proteção contra Malware para S3. Se você tentar ativar o plano de proteção imediatamente após criar o perfil, a validação poderá falhar.
- Para implantações de infraestrutura como código (IaC), GuardDuty recomenda declarar uma dependência de recursos para garantir que a função do IAM alcance uma eventual consistência.

  Para exemplos de modelos sobre como fazer isso, consulte GuardDuty GitHubrepositório.

Cross-region capacitação

Certifique-se de que seu bucket do Amazon S3 esteja na mesma região em que você está habilitando a proteção contra malware para o S3. GuardDuty

Etapas para habilitar a proteção contra malware para S3

Esta seção lista as etapas que você pode seguir após ativar a Proteção contra Malware para S3 em um bucket. As etapas a seguir estão listadas em uma ordem que ajudará você a navegar pelas próximas etapas:

A seguir, depois de ativar o Proteção contra Malware para S3 em seu bucket

1. Adicione política de recursos de controle de acesso baseado em tags (TBAC) — Ao ativar a marcação, antes que um objeto seja carregado no bucket selecionado, certifique-se de adicionar a política TBAC ao recurso do bucket do S3. Para obter mais informações, consulte Adicionando TBAC ao recurso do bucket do S3.
2. Monitore o status do plano de proteção contra malware — monitore a coluna Status de cada bucket protegido. Para obter informações sobre possíveis status e o que eles significam, consulteVisualizar e entender o status do bucket protegido.
3. Inicie um escaneamento escolhendo uma das seguintes opções:
   - Faça upload de um objeto:
     1. Abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
     2. Faça upload de um arquivo para seu bucket do S3 ou para o prefixo de objeto para o qual você habilitou este atributo. Para etapas para fazer o upload de um arquivo, consulte Fazer upload de um objeto para o seu bucket no Guia do usuário do Amazon S3.
   - Inicie uma varredura por solicitação: On-demand Verificação de malware S3 GuardDuty
4. Monitore o status e o resultado da verificação de objetos do S3 — Essa etapa inclui informações sobre como verificar o status da verificação de malware do objeto do S3.

Ativou a proteção contra malware GuardDuty e o S3	Habilitada Proteção contra malware para S3 somente
• Quando GuardDuty ativado, ele pode gerar o Tipo de descoberta da Proteção contra malware para S3 para indicar a presença de malware no objeto S3 escaneado. • Você pode verificar potencialmente o resultado da verificação de objetos do S3 usando uma ou mais opções emMonitoran	Você pode verificar potencialmente o resultado da verificação de objetos do S3 usando uma ou mais opções emMonitoran do verificações de objetos do S3 na Proteção contra Malware para S3. Isso inclui o uso da Amazon EventBridge, CloudWatch métricas

Ativou a proteção contra malware GuardDuty e o S3	Habilitada Proteção contra malware para S3 somente
do verificações de objetos do S3 na Proteção contra Malware para S3. Isso inclui o uso da Amazon EventBridge, CloudWatch métricas para o plano de proteção contra malware e a marcação de objetos escaneados.	para o plano de proteção contra malware e a marcação de objetos escaneados.

On-demand Verificação de malware S3 GuardDuty

GuardDuty O Malware Protection for S3 monitora continuamente novos uploads do S3. Para objetos que existiam antes de ativar a proteção, ou para verificar novamente objetos escaneados anteriormente, você pode iniciar a verificação de malware sob demanda do S3 depois de habilitar o plano de proteção contra GuardDuty malware para seu bucket.

On-demand o escaneamento de malware usa a função IAM do Plano de Proteção contra Malware para acessar objetos e aplicar a configuração. A verificação substituirá qualquer prefixo configurado no Plano de Proteção contra Malware do bucket.

> **Note**
>
> A cota do Malware Protection for S3 se aplica à verificação de malware sob demanda. Para obter mais informações, consulteQuotas na Proteção contra malware para o S3.
> Para obter mais informações sobre a definição de preços, consulte Preço e custo de uso da Proteção contra Malware para S3.

Pré-requisitos

Antes de iniciar uma verificação de malware sob demanda, sua conta deve atender aos seguintes pré-requisitos:

- A proteção contra malware para S3 está ativada no bucket de destino. Consulte Configurando a proteção contra malware para S3 para seu bucket para obter mais informações.

- A AWS política gerenciada: AmazonGuardDutyFullAccess_v2 (recomendado) política é anexada ao usuário do IAM ou à função do IAM que invoca a API.

Inicie a verificação de malware sob demanda

Use a operação SendObjectMalwareScanda API, que exige o caminho do objeto S3 como entrada.

API/CLI

Você pode digitalizar a versão mais recente do objeto ou especificar uma versão específica para digitalizar.

Para digitalizar uma versão específica de um objeto:

```
aws guardduty send-object-malware-scan --s3-object '{"Bucket":
 "amzn-s3-demo-bucket", "Key": "APKAEIBAERJR2EXAMPLE", "VersionId":
 "d41d8cd98f00b204e9800998eEXAMPLE"}'
```

Para escanear a versão mais recente de um objeto:

```
aws guardduty send-object-malware-scan --s3-object '{"Bucket": "amzn-s3-demo-
bucket", "Key": "APKAEIBAERJR2EXAMPLE"}'
```

Important

Uma chamada de API bem-sucedida confirma que a solicitação de verificação foi aceita. No entanto, é importante monitorar os resultados da verificação para garantir a conclusão bem-sucedida e identificar quaisquer problemas, como erros ao acessar o objeto. Para obter mais informações, consulte Monitorando verificações de objetos do S3 na Proteção contra Malware para S3.

Usando controle de acesso baseado em tags (TBAC) com proteção contra malware para S3

Ao habilitar a Proteção contra Malware para S3 para o seu bucket, você pode optar por habilitar a marcação. Depois de tentar escanear um objeto S3 recém-carregado no bucket selecionado,

GuardDuty adiciona uma tag ao objeto escaneado para fornecer o status da verificação de malware. Há um custo de uso direto associado quando você ativa a marcação. Para obter mais informações, consulte Preço e custo de uso da Proteção contra Malware para S3.

GuardDuty usa uma tag predefinida com a chave como `GuardDutyMalwareScanStatus` e o valor como um dos status de verificação de malware. Para obter informações sobre esses valores, consulte the section called “Status de verificação potencial do objeto S3 e status do resultado”.

Considerações GuardDuty para adicionar uma tag ao seu objeto do S3:

- Por padrão. você pode associar até 10 tags a um objeto. Para obter informações, consulte Categorizando o armazenamento usando tags no Guia do usuário do Amazon S3.

  Se todas as 10 tags já estiverem em uso, não GuardDuty será possível adicionar a tag predefinida ao objeto digitalizado. GuardDuty também publica o resultado da verificação no seu barramento de EventBridge eventos padrão. Para obter mais informações, consulte Monitoramento de escaneamentos de objetos do S3 com a Amazon EventBridge.
- Quando a função do IAM selecionada não inclui a permissão GuardDuty para marcar o objeto do S3, mesmo com a marcação ativada para seu bucket protegido, não GuardDuty será possível adicionar uma tag a esse objeto escaneado do S3. Para obter mais informações sobre como criar uma permissão do perfil do IAM para marcação de tag, consulte Criar ou atualizar a política do perfil do IAM.

  GuardDuty também publica o resultado da verificação no seu barramento de EventBridge eventos padrão. Para obter mais informações, consulte Monitoramento de escaneamentos de objetos do S3 com a Amazon EventBridge.

Adicionando TBAC ao recurso do bucket do S3

Você pode usar as políticas de recursos do bucket do S3 para gerenciar o controle de acesso baseado em tags (TBAC) para seus objetos do S3. Você pode fornecer acesso a usuários específicos para acessar e ler o objeto S3. Se você tiver uma organização que foi criada usando AWS Organizations, você deve garantir que ninguém possa modificar as tags adicionadas por GuardDuty. Para obter mais informações, consulte Como evitar que as tags sejam modificadas, exceto por responsáveis autorizados, no Guia do AWS Organizations usuário. O exemplo usado no tópico vinculado menciona `ec2`. Ao usar esse exemplo, substitua *`ec2`* por `s3`.

A lista a seguir explica o que você pode fazer usando o TBAC:

- Impeça que todos os usuários, exceto a entidade principal do serviço de Proteção de Malware para S3, leiam os objetos do S3 que ainda não estão marcados com o seguinte par de valor chave de tag:

  `GuardDutyMalwareScanStatus:`*`Potential key value`*

- Permita apenas GuardDuty adicionar a chave de tag `GuardDutyMalwareScanStatus` com valor como resultado da digitalização a um objeto S3 digitalizado. O modelo de política a seguir pode permitir que usuários específicos que tenham acesso possam potencialmente substituir o par chave-valor da tag.

Política de recursos do bucket do S3 do exemplo

Substitua os seguintes valores de espaços reservados na política de exemplo:

- *`IAM-role-name`*- Forneça a função do IAM que você usou para configurar a proteção contra malware para S3 em seu bucket.
- *`555555555555`*- Forneça o Conta da AWS associado ao bucket protegido.
- *`amzn-s3-demo-bucket`*- Forneça o nome do bucket protegido.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [{
            "Sid": "NoReadUnlessClean",
            "Effect": "Deny",
            "NotPrincipal": {
                "AWS": [
                "arn:aws:sts::555555555555:assumed-role/IAM-role-name/
GuardDutyMalwareProtection",
                "arn:aws:iam::555555555555:role/IAM-role-name"
                ]
            },
            "Action": [
                "s3:GetObject",
                "s3:GetObjectVersion"
            ],
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*",
            "Condition": {
```

```
                "StringNotEquals": {
                    "s3:ExistingObjectTag/GuardDutyMalwareScanStatus":
 "NO_THREATS_FOUND"
                }
            }
        },
        {
            "Sid": "OnlyGuardDutyCanTagScanStatus",
            "Effect": "Deny",
            "NotPrincipal": {
                "AWS": [
                    "arn:aws:sts::555555555555:assumed-role/IAM-role-name/
GuardDutyMalwareProtection",
                    "arn:aws:iam::555555555555:role/IAM-role-name"
                ]
            },
            "Action": "s3:PutObjectTagging",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*",
            "Condition": {
                "ForAnyValue:StringEquals": {
                    "s3:RequestObjectTagKeys": "GuardDutyMalwareScanStatus"
                }
            }
        }
    ]
}
```

Para obter mais informações sobre como marcar seu recurso do S3, consulte Políticas de marcação e controle de acesso.

Visualizar e entender o status do bucket protegido

Depois de habilitar a Proteção contra Malware para S3 para um bucket, o status indica se o recurso está configurado e funcionando conforme esperado. Esse status está associado a um identificador (ID) exclusivo do plano de Proteção contra Malware. GuardDuty cria esse ID no momento da ativação do recurso.

Use o procedimento a seguir para visualizar o status do bucket protegido:

1. Faça login no Console de gerenciamento da AWS e abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.

2. No painel de navegação, escolha Proteção contra Malware para S3.
3. Na tabela Buckets protegidos, visualize a coluna Status correspondente para seu bucket do S3.

A tabela a seguir lista e descreve os valores de status associados ao recurso do plano de Proteção contra Malware. Ao entender o que esses status significam para seu bucket protegido, você pode garantir melhor que ele GuardDuty inicie uma verificação automática de malware quando um objeto é carregado.

Status	Description
Ativo	Seu bucket do S3 foi configurado com a Proteção contra Malware para S3 com sucesso. Quando o status é Ativo, as alterações no perfil do IAM (exclusão ou modificação de permissões) não vão atualizar o status para Aviso ou Erro. Recomendamos monitorar o status da verificação continuamente usando qualquer um dos métodos descritos em Monitoramento de verificações de objetos de S3.
Aviso*	A Proteção contra Malware para S3 foi projetada para não ser afetada quando um aviso aparecer. Quando GuardDuty percebe um novo objeto do S3, ele inicia uma verificação de malware. Depois de iniciar a verificação com sucesso, o valor da coluna Status pode levar alguns minutos para ser alterado para Ativo. Você receberá uma EventBridge notificação após a atualização do valor da coluna Status.
Erro*	Seu bucket não está protegido. Nenhuma das verificações de malware associadas a esse bucket do S3 será concluída. Pode haver uma ou mais causas possíveis.

* Para obter informações sobre possíveis problemas e as etapas correspondentes para resolvê-los, consulteSolução de problemas do status do plano de proteção contra malware.

Monitorando verificações de objetos do S3 na Proteção contra Malware para S3

Ao usar o Malware Protection for S3 com um ID de GuardDuty detector, se seu objeto do Amazon S3 for potencialmente malicioso GuardDuty , ele será gerado. Tipo de descoberta da Proteção contra malware para S3 Usando o GuardDuty console e as APIs, você pode visualizar as descobertas geradas. Para obter informações sobre como entender esse tipo de descoberta, consulteDetalhes da descoberta.

Ao usar o Malware Protection for S3 sem habilitar GuardDuty (sem ID de detector), mesmo quando seu objeto escaneado do Amazon S3 é potencialmente malicioso GuardDuty , não é possível gerar nenhuma descoberta.

Conteúdo

- Status de verificação potencial do objeto S3 e status do resultado
- Monitoramento de escaneamentos de objetos do S3 com a Amazon EventBridge
- Monitoramento de escaneamentos de objetos do S3 com tags gerenciadas GuardDuty
- Métricas de status de escaneamento de objetos do S3 em CloudWatch

Status de verificação potencial do objeto S3 e status do resultado

Esta seção explica os possíveis valores de status de verificação de objetos do S3 e os valores do resultado da verificação.

O status de verificação de objetos do S3 indica o status de verificação de malware, como concluído, ignorado ou falhado.

O status do resultado de verificação de malware do objeto S3 indica o resultado de verificação com base no valor do status de verificação. O valor de status de cada resultado de verificação de malware é mapeado para um status de de verificação.

A lista a seguir fornece os valores potenciais do resultado da varredura de objetos do S3. Se você ativou a marcação, você pode monitorar o resultado da verificação porUso de marcações de objeto S3. Após a verificação, o valor da marcação terá um dos seguintes valores de resultado da verificação.

Valores de status do resultado da verificação de malware em potencial do objeto S3

- `NO_THREATS_FOUND`— não GuardDuty detectou nenhuma ameaça potencial associada ao objeto escaneado.
- `THREATS_FOUND`— GuardDuty detectou uma ameaça potencial associada ao objeto escaneado.
- `UNSUPPORTED`— Existem alguns motivos pelos quais a Proteção de Malware para S3 pulará uma verificação. Os possíveis motivos incluem arquivo protegido por senha, arquivamentos com taxas de compactação extremamente altas, Cotas de Proteção contra malware para o S3 e suporte para determinados atributos do Amazon S3 que podem estar indisponíveis. Para obter mais informações, consulte Capacidades da proteção contra malware para S3.
- `ACCESS_DENIED`— não GuardDuty consigo acessar esse objeto para digitalização. Verifique as permissões do perfil do IAM associadas a esse bucket. Para obter mais informações, consulte Criar ou atualizar a política do perfil do IAM.

  Se você ativou a marcação de objetos do S3 após a verificação, consulte. Solução de problemas de falhas na marcação pós-verificação do objeto S3
- `FAILED`— não é GuardDuty possível realizar a verificação de malware neste objeto devido a um erro interno.

A lista a seguir fornece possíveis valores de status de verificação de objetos do S3 e seu mapeamento para o resultado da verificação de objetos do S3.

Valores de status de verificação potencial do objeto S3

- Concluído — O verificação foi concluído com êxito e indica se o objeto S3 tem malware. Nesse caso, o valor potencial do resultado da verificação de objetos do S3 pode ser `THREATS_FOUND` ou`NO_THREATS_FOUND`.
- Ignorado — GuardDuty ignora uma verificação de malware ao escanear esse objeto do S3, não é compatível com o Malware Protection for S3 ou GuardDuty não tem acesso ao objeto do S3 carregado no bucket selecionado.

  Nesse caso, o valor potencial do resultado da verificação de objetos do S3 pode ser `UNSUPPORTED` ou`ACCESS_DENIED`.

  GuardDuty também pulará a verificação se a função do IAM necessária for excluída.

- Falha — Semelhante ao valor do resultado da verificação de objetos do S3`FAILED`, esse status de verificação significa que não GuardDuty foi possível realizar a verificação de malware no objeto do S3 devido a um erro interno.

Quando o status do escaneamento é`SKIPPED`, a EventBridge notificação para o resultado do escaneamento de objetos do S3 inclui um `statusReasons` campo dentro`scanResultDetails`. Esse campo é uma lista de sequências de caracteres que fornece o motivo específico pelo qual a verificação foi ignorada. A tabela a seguir descreve os `statusReasons` valores possíveis.

Motivo do status	Status do resultado da verificação	Description
`UNAUTHORIZED_TO_GET_OBJECT`	`ACCESS_DENIED`	O Malware Protection for S3 não tem permissão para ler o objeto S3, ou o objeto S3 não existe. Verifique se a função do IAM associada ao bucket protegido tem as permissões necessárias e se qualquer AWS KMS política de bucket permite que a função decodifique objetos.
`UNAUTHORIZED_TO_ASSUME_ROLE`	`ACCESS_DENIED`	O Malware Protection for S3 não pode assumir a função do IAM configurada para o bucket protegido. Verifique se a política de confiança da função permite que o Malware Protection for S3 assuma a função.
`SSE_C_ENCRYPTED_OBJECT`	`ACCESS_DENIED`	O objeto S3 é criptografado com uma chave de criptografia fornecida pelo cliente (). SSE-C GuardDuty não consigo acessar objetos criptografados com SSE-C. Para obter mais informações, consulte Suportabilidade dos atributos do Amazon S3.
`OBJECT_E_TAG_CHANGED`	`ACCESS_DENIED`	A ETag do objeto S3 mudou entre o momento em que a varredura foi iniciada e a GuardDuty

Motivo do status	Status do resultado da verificação	Description
		tentativa de ler o objeto. O upload subsequente ou a nova versão serão digitalizados.
BUCKET_NOT_FOUND	ACCESS_DENIED	O bucket do S3 associado à verificação não existe mais.
UNSUPPORTED_STORAGE_CLASS	UNSUPPORTED	O objeto S3 usa uma classe de armazenamento que não é compatível com o Malware Protection for S3. Para obter mais informações, consulte Suportabilidade dos atributos do Amazon S3.
OBJECT_SIZE_LIMIT_EXCEEDED	UNSUPPORTED	O tamanho do objeto do S3 excede o limite máximo de tamanho de arquivo do Malware Protection for S3. Para obter mais informações, consulte Cotas de Proteção contra malware para o S3.
PASSWORD_PROTECTED	UNSUPPORTED	O objeto é protegido por senha.
EXTRACTED_FILE_LIMIT_EXCEEDED	UNSUPPORTED	O arquivo contém mais arquivos do que o limite máximo permitido. Para obter mais informações, consulte Cotas de Proteção contra malware para o S3.
EXTRACTED_LEVEL_LIMIT_EXCEEDED	UNSUPPORTED	O arquivo excede a profundidade máxima de aninhamento permitida.
EXTRACTED_BYTE_LIMIT_EXCEEDED	UNSUPPORTED	O conteúdo do arquivo extraído excede o tamanho máximo de bytes permitido. Para obter mais informações, consulte Cotas de Proteção contra malware para o S3.

Motivo do status	Status do resultado da verificação	Description
`EXTRACTION_RATIO_LIMIT_EXCEEDED`	`UNSUPPORTED`	O arquivo tem uma taxa de compressão extremamente alta que excede o limite permitido. Para obter mais informações, consulte Cotas de Proteção contra malware para o S3.

Monitoramento de escaneamentos de objetos do S3 com a Amazon EventBridge

EventBridgeA Amazon é um serviço de ônibus de eventos sem servidor que facilita a conexão de seus aplicativos com dados de várias fontes. EventBridge fornece um fluxo de dados em tempo real de seus próprios aplicativos, aplicativos Software-as-a-Service (SaaS) e AWS serviços e encaminha esses dados para destinos como o Lambda. Isso permite monitorar eventos que ocorram em serviços e criem arquiteturas orientadas a eventos. Para obter mais informações, consulte o Guia EventBridge do usuário da Amazon.

Como conta do proprietário de um bucket do S3 protegido com o Malware Protection for S3, GuardDuty publica EventBridge notificações no barramento de eventos padrão nos seguintes cenários:

- Alterações no status dos recursos do plano de proteção contra malware para qualquer um dos seus buckets protegidos. Para obter mais informações sobre vários status, consulte Visualizar e entender o status do bucket protegido.

  Para configurar a regra Amazon EventBridge (EventBridge) para o status do recurso, consulteStatus do recurso do plano de proteção contra malware.
- O resultado da verificação de objetos do S3 é publicado no seu barramento de EventBridge eventos padrão.

  O campo `s3Throttled` indica se houve ou não um atraso no upload ou na recuperação do armazenamento dos Amazon S3. O valor `true` indica que houve um atraso e `false` indica que não houve atraso.

Se `s3Throttled` for `true` para o resultado da verificação, o Amazon S3 recomenda configurar prefixos de uma forma que ajude a reduzir as transações por segundo (TPS) para cada prefixo. Para obter mais informações, consulte Padrões de Design de Práticas Recomendadas: Otimizando a Performance do Amazon S3 no Guia de Usuário do Amazon S3.

Para configurar a regra Amazon EventBridge (EventBridge) para os resultados de escaneamento de objetos do S3, consulteResultado da verificação de objetos do S3.

- Há um evento de falha na etiqueta pós-verificação devido aos seguintes motivos:
  - Seu perfil do IAM não tem permissões para marcar o objeto.

    O Adicionar permissões de política do IAM modelo inclui a permissão GuardDuty para marcar um objeto.
  - O recurso ou objeto do bucket especificado no perfil do IAM não existe mais.
  - O objeto S3 associado já atingiu o limite máximo de marcações. Para obter informações, sobre o limite de marcações, consulte Categorizando o armazenamento usando marcações no Guia do usuário do Amazon S3.

  Para configurar a regra Amazon EventBridge (EventBridge) para os eventos de falha da tag pós-digitalização, consultePost-scan eventos de falha de tag.

Configurar EventBridge regras

Você pode configurar EventBridge regras em sua conta para enviar o status do recurso, os eventos de falha da tag pós-escaneamento ou o resultado do escaneamento de objetos do S3 para outra pessoa. AWS service (Serviço da AWS) Como conta de GuardDuty administrador delegado, você receberá a notificação de status do recurso do plano de Proteção contra Malware quando houver uma alteração no status.

O EventBridge preço padrão será aplicado. Para obter mais informações, consulte os EventBridge preços da Amazon.

Todos os valores que aparecem em *`red`* são espaços reservados para o exemplo. Esses valores mudarão com base nos valores da sua conta e na detecção ou não de malware.

Tópicos

- Status do recurso do plano de proteção contra malware
- Resultado da verificação de objetos do S3

- Post-scan eventos de falha de tag

Status do recurso do plano de proteção contra malware

Você pode criar um padrão de EventBridge evento com base nos seguintes cenários:

Valores potenciais do **`tipo de detalhe`**

- `"GuardDuty Malware Protection Resource Status Active"`
- `"GuardDuty Malware Protection Resource Status Warning"`
- `"GuardDuty Malware Protection Resource Status Error"`

Padrão de evento

```
{
      "detail-type": ["potential detail-type"],
      "source": ["aws.guardduty"]
}
```

Exemplo de esquema de notificação para **`GuardDuty Malware Protection Resource Status Active`**:

```
{
    "version": "0",
    "id": "6a7e8feb-b491-4cf7-a9f1-bf3703467718",
    "detail-type": "GuardDuty Malware Protection Resource Status Active",
    "source": "aws.guardduty",
    "account": "111122223333",
    "time": "2017-12-22T18:43:48Z",
    "region": "us-east-1",
    "resources": ["arn:aws:guardduty:us-east-1:111122223333:malware-protection-plan/
b4c7f464ab3a4EXAMPLE"],
    "detail": {
        "schemaVersion": "1.0",
        "eventTime": "2024-02-28T01:01:01Z",
        "s3BucketDetails": {
            "bucketName": "amzn-s3-demo-bucket"
        },
        "resourceStatus": "ACTIVE"
    }
```

```
}
```

Exemplo de esquema de notificação para **`GuardDuty Malware Protection Resource Status Warning`**:

```
{
    "version": "0",
    "id": "6a7e8feb-b491-4cf7-a9f1-bf3703467718",
    "detail-type": "GuardDuty Malware Protection Resource Status warning",
    "source": "aws.guardduty",
    "account": "111122223333",
    "time": "2017-12-22T18:43:48Z",
    "region": "us-east-1",
    "resources": ["arn:aws:guardduty:us-east-1:111122223333:malware-protection-plan/
b4c7f464ab3a4EXAMPLE"],
    "detail": {
        "schemaVersion": "1.0",
        "eventTime": "2024-02-28T01:01:01Z",
        "s3BucketDetails": {
            "bucketName": "amzn-s3-demo-bucket"
        },
        "resourceStatus": "WARNING",
        "statusReasons": [
         {
            "code": "INSUFFICIENT_TEST_OBJECT_PERMISSIONS"
         }
        ]
    }
}
```

Exemplo de esquema de notificação para **`GuardDuty Malware Protection Resource Status Error`**:

```
{
    "version": "0",
    "id": "fc7a35b7-83bd-3c1f-ecfa-1b8de9e7f7d2",
    "detail-type": "GuardDuty Malware Protection Resource Status Error",
    "source": "aws.guardduty",
    "account": "111122223333",
    "time": "2017-12-22T18:43:48Z",
    "region": "us-east-1",
```

```
    "resources": ["arn:aws:guardduty:us-east-1:111122223333:malware-protection-plan/
b4c7f464ab3a4EXAMPLE"],
    "detail": {
        "schemaVersion": "1.0",
        "eventTime": "2024-02-28T01:01:01Z",
        "s3BucketDetails": {
            "bucketName": "amzn-s3-demo-bucket"
        },
        "resourceStatus": "ERROR",
        "statusReasons": [
        {
            "code": "EVENTBRIDGE_MANAGED_EVENTS_DELIVERY_DISABLED"
        }
       ]
    }
}
```

Com base no motivo por trás do `resourceStatus`ERROR, o `statusReasons` valor será preenchido.

Para obter informações sobre as etapas de solução de problemas dos seguintes avisos e erros, consulteSolução de problemas do status do plano de proteção contra malware.

Resultado da verificação de objetos do S3

```
{
  "detail-type": ["GuardDuty Malware Protection Object Scan Result"],
  "source": ["aws.guardduty"]
}
```

Quando `scanStatus` for`SKIPPED`, `scanResultDetails` inclui um `statusReasons` campo que fornece o motivo específico pelo qual o escaneamento foi ignorado. Para obter informações sobre os valores possíveis, consulteStatus de verificação potencial do objeto S3 e status do resultado.

Exemplo de esquema de notificação para **`NO_THREATS_FOUND`**:

```
{
    "version": "0",
    "id": "72c7d362-737a-6dce-fc78-9e27a0171419",
    "detail-type": "GuardDuty Malware Protection Object Scan Result",
    "source": "aws.guardduty",
    "account": "111122223333",
```

```
    "time": "2024-02-28T01:01:01Z",
    "region": "us-east-1",
    "resources": ["arn:aws:guardduty:us-east-1:111122223333:malware-protection-plan/
b4c7f464ab3a4EXAMPLE"],
    "detail": {
        "schemaVersion": "1.0",
        "scanStatus": "COMPLETED",
        "resourceType": "S3_OBJECT",
        "s3ObjectDetails": {
            "bucketName": "amzn-s3-demo-bucket",
            "objectKey": "APKAEIBAERJR2EXAMPLE",
            "eTag": "ASIAI44QH8DHBEXAMPLE",
            "versionId" : "d41d8cd98f00b204e9800998eEXAMPLE",
            "s3Throttled": false
        },
        "scanResultDetails": {
            "scanResultStatus": "NO_THREATS_FOUND",
            "threats": null,
            "statusReasons": null
        }
    }
}
```

Exemplo de esquema de notificação para **THREATS_FOUND**:

```
{
    "version": "0",
    "id": "72c7d362-737a-6dce-fc78-9e27a0171419",
    "detail-type": "GuardDuty Malware Protection Object Scan Result",
    "source": "aws.guardduty",
    "account": "111122223333",
    "time": "2024-02-28T01:01:01Z",
    "region": "us-east-1",
    "resources": ["arn:aws:guardduty:us-east-1:111122223333:malware-protection-plan/
b4c7f464ab3a4EXAMPLE"],
    "detail": {
        "schemaVersion": "1.0",
        "scanStatus": "COMPLETED",
        "resourceType": "S3_OBJECT",
        "s3ObjectDetails": {
            "bucketName": "amzn-s3-demo-bucket",
            "objectKey": "APKAEIBAERJR2EXAMPLE",
            "eTag": "ASIAI44QH8DHBEXAMPLE",
```

```
            "versionId" : "d41d8cd98f00b204e9800998eEXAMPLE",
            "s3Throttled": false
        },
        "scanResultDetails": {
            "scanResultStatus": "THREATS_FOUND",
            "threats": [
                {
                    "name": "EICAR-Test-File (not a virus)",
                    "source": "AMAZON",
                    "itemDetails": [{
                        "hash":
 "e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855",
                        "itemPath": "APKAEIBAERJR2EXAMPLE"
                    }]
                }
            ],
            "statusReasons": null
        }
    }
}
```

> **Note**
>
> O campo `scanResultDetails.Threats` contém apenas uma ameaça. Por padrão, a verificação do Proteção contra Malware para S3 relata a primeira ameaça detectada. Depois disso, o `scanStatus` é definido como`COMPLETED`.

Exemplo de esquema de notificação para o status do resultado da verificação **`UNSUPPORTED`** (ignorado):

```
{
    "version": "0",
    "id": "72c7d362-737a-6dce-fc78-9e27a0EXAMPLE",
    "detail-type": "GuardDuty Malware Protection Object Scan Result",
    "source": "aws.guardduty",
    "account": "111122223333",
    "time": "2024-02-28T01:01:01Z",
    "region": "us-east-1",
    "resources": ["arn:aws:guardduty:us-east-1:111122223333:malware-protection-plan/
b4c7f464ab3a4EXAMPLE"],
    "detail": {
```

```
        "schemaVersion": "1.0",
        "scanStatus": "SKIPPED",
        "resourceType": "S3_OBJECT",
        "s3ObjectDetails": {
            "bucketName": "amzn-s3-demo-bucket",
            "objectKey": "APKAEIBAERJR2EXAMPLE",
            "eTag": "ASIAI44QH8DHBEXAMPLE",
            "versionId" : "d41d8cd98f00b204e9800998eEXAMPLE",
            "s3Throttled": false
        },
        "scanResultDetails": {
            "scanResultStatus": "UNSUPPORTED",
            "threats": null,
            "statusReasons": ["PASSWORD_PROTECTED"]
        }
    }
}
```

Exemplo de esquema de notificação para o status do resultado da verificação **`ACCESS_DENIED`** (ignorado):

```
{
    "version": "0",
    "id": "72c7d362-737a-6dce-fc78-9e27a0EXAMPLE",
    "detail-type": "GuardDuty Malware Protection Object Scan Result",
    "source": "aws.guardduty",
    "account": "111122223333",
    "time": "2024-02-28T01:01:01Z",
    "region": "us-east-1",
    "resources": ["arn:aws:guardduty:us-east-1:111122223333:malware-protection-plan/
b4c7f464ab3a4EXAMPLE"],
    "detail": {
        "schemaVersion": "1.0",
        "scanStatus": "SKIPPED",
        "resourceType": "S3_OBJECT",
        "s3ObjectDetails": {
            "bucketName": "amzn-s3-demo-bucket",
            "objectKey": "APKAEIBAERJR2EXAMPLE",
            "eTag": "ASIAI44QH8DHBEXAMPLE",
            "versionId" : "d41d8cd98f00b204e9800998eEXAMPLE",
            "s3Throttled": false
        },
        "scanResultDetails": {
```

```
            "scanResultStatus": "ACCESS_DENIED",
            "threats": null,
            "statusReasons": ["SSE_C_ENCRYPTED_OBJECT"]
        }
    }
}
```

Exemplo de esquema de notificação para o status do resultado da verificação **`FAILED`**:

```
{
    "version": "0",
    "id": "72c7d362-737a-6dce-fc78-9e27a0EXAMPLE",
    "detail-type": "GuardDuty Malware Protection Object Scan Result",
    "source": "aws.guardduty",
    "account": "111122223333",
    "time": "2024-02-28T01:01:01Z",
    "region": "us-east-1",
    "resources": ["arn:aws:guardduty:us-east-1:111122223333:malware-protection-plan/
b4c7f464ab3a4EXAMPLE"],
    "detail": {
        "schemaVersion": "1.0",
        "scanStatus": "FAILED",
        "resourceType": "S3_OBJECT",
        "s3ObjectDetails": {
            "bucketName": "amzn-s3-demo-bucket",
            "objectKey": "APKAEIBAERJR2EXAMPLE",
            "eTag": "ASIAI44QH8DHBEXAMPLE",
            "versionId" : "d41d8cd98f00b204e9800998eEXAMPLE",
            "s3Throttled": false
        },
        "scanResultDetails": {
            "scanResultStatus": "FAILED",
            "threats": null,
            "statusReasons": null
        }
    }
}
```

Post-scan eventos de falha de tag

Padrão de evento:

```
{
```

```
      "detail-type": "GuardDuty Malware Protection Post Scan Action Failed",
      "source": "aws.guardduty"
 }
```

Exemplo de esquema de notificação para **`ACCESS_DENIED`**:

```
{
    "version": "0",
    "id": "746acd83-d75c-5b84-91d2-dad5f13ba0d7",
    "detail-type": "GuardDuty Malware Protection Post Scan Action Failed",
    "source": "aws.guardduty",
    "account": "111122223333",
    "time": "2024-06-10T16:16:08Z",
    "region": "us-east-1",
    "resources": ["arn:aws:guardduty:us-east-1:111122223333:malware-protection-plan/
b4c7f464ab3a4EXAMPLE"],
    "detail": {
        "schemaVersion": "1.0",
        "eventTime": "2024-06-10T16:16:08Z",
        "s3ObjectDetails": {
            "bucketName": "amzn-s3-demo-bucket",
            "objectKey": "2024-03-10-16-16-00-7D723DE8DBE9Y2E0",
            "eTag": "0e9eeec810ad8b61d69112c15c2a5hb6",
            "versionId" : "d41d8cd98f00b204e9800998eEXAMPLE",
            "s3Throttled": false
        },
        "postScanActions": [{
            "actionType": "TAGGING",
            "failureReason": "ACCESS_DENIED"
        }]
    }
}
```

Exemplo de esquema de notificação para **`MAX_TAG_LIMIT_EXCEEDED`**:

```
{
    "version": "0",
    "id": "746acd83-d75c-5b84-91d2-dad5f13ba0d7",
    "detail-type": "GuardDuty Malware Protection Post Scan Action Failed",
    "source": "aws.guardduty",
    "account": "111122223333",
    "time": "2024-06-10T16:16:08Z",
    "region": "us-east-1",
```

```
    "resources": ["arn:aws:guardduty:us-east-1:111122223333:malware-protection-plan/
b4c7f464ab3a4EXAMPLE"],
    "detail": {
        "schemaVersion": "1.0",
        "eventTime": "2024-06-10T16:16:08Z",
        "s3ObjectDetails": {
            "bucketName": "amzn-s3-demo-bucket",
            "objectKey": "2024-03-10-16-16-00-7D723DE8DBE9Y2E0",
            "eTag": "0e9eeec810ad8b61d69112c15c2a5hb6",
            "versionId" : "d41d8cd98f00b204e9800998eEXAMPLE",
            "s3Throttled": false
        },
        "postScanActions": [{
            "actionType": "TAGGING",
            "failureReason": "MAX_TAG_LIMIT_EXCEEDED"
        }]
    }
}
```

Para solucionar esses motivos de falha, consulteSolução de problemas de falhas na marcação pós-verificação do objeto S3.

Monitoramento de escaneamentos de objetos do S3 com tags gerenciadas GuardDuty

Use a opção de habilitar marcação para que GuardDuty você possa adicionar tags ao seu objeto Amazon S3 depois de concluir a verificação de malware.

Considerações para ativar a marcação

- Há um custo de uso associado ao marcar GuardDuty seus objetos do S3. Para obter mais informações, consulte Preço e custo de uso da Proteção contra Malware para S3.
- Você deve manter as permissões de marcação necessárias para sua função preferida do IAM associada a esse bucket; caso contrário, não GuardDuty poderá adicionar tags aos seus objetos digitalizados. O perfil do IAM já inclui as permissões para adicionar marcações aos objetos verificados do S3. Para obter mais informações, consulte Criar ou atualizar a política do perfil do IAM.
- Por padrão, você pode associar até 10 marcações a um objeto S3. Para obter mais informações, consulte Usando controle de acesso baseado em tags (TBAC).

Depois de ativar a marcação para um bucket do S3 ou prefixos específicos, qualquer objeto recém-carregado que for verificado terá uma marcação associada no seguinte formato de par de valores-chave:

`GuardDutyMalwareScanStatus:`*`Scan-Result-Status`*

Para obter informações sobre possíveis valores de marcação, consulte[Status de verificação potencial do objeto S3 e status do resultado](#).

Solução de problemas de falhas na marcação pós-verificação de objetos do S3 na Proteção contra Malware para S3

Esta seção se aplica a você somente se você estiver [Ativar marcação para objetos verificados](#) em seu bucket protegido.

Ao GuardDuty tentar adicionar uma tag ao objeto escaneado do S3, a ação de marcar pode resultar em uma falha. Os possíveis motivos pelos quais isso pode acontecer com seu bucket são `ACCESS_DENIED` `MAX_TAG_LIMIT_EXCEEDED` e. Use os tópicos a seguir para entender os possíveis motivos desses motivos de falha na marcação pós-verificação e solucioná-los.

ACCESS_DENIED

A lista a seguir fornece possíveis motivos que podem causar esse problema:

- A função do IAM usada para esse bucket protegido do S3 não tem a AllowPostScanTagpermissão. Verifique se o perfil do IAM associada usa essa política de bucket. Para obter mais informações, consulte [Criar ou atualizar a política do perfil do IAM](#).
- A política de bucket protegido do S3 não permite GuardDuty adicionar tags a esse objeto.
- O objeto do S3 verificado não existe mais.

MAX_TAG_LIMIT_EXCEDIDO

Por padrão, você pode associar até 10 marcações a um objeto S3. Para obter mais informações, consulte Considerações GuardDuty para adicionar uma tag ao seu objeto do S3 em. [Ativar marcação para objetos verificados](#)

Métricas de status de escaneamento de objetos do S3 em CloudWatch

Você pode monitorar GuardDuty o uso CloudWatch, que coleta dados brutos e os processa em métricas legíveis e quase em tempo real. Essas estatísticas são mantidas por um período de 15

meses para que seja possível acessar informações históricas e obter uma perspectiva melhor sobre como a Proteção contra Malware para S3 está indo. Você também pode definir alarmes que observam determinados limites e enviam notificações ou realizam ações quando esses limites são atingidos. Para obter mais informações, consulte o Guia CloudWatch do usuário da Amazon.

As CloudWatch métricas do Malware Protection for S3 estão disponíveis no nível do recurso. Você pode consultar essas métricas para cada recurso protegido separadamente. As métricas estão no namespace `AWS/GuardDuty/MalwareProtection`. Você pode configurar alarmes em recursos específicos para monitorar a postura de segurança.

Métricas de status da verificação de malware

Métrica	Descrição
`CompletedScanCount`	O número de verificações de malware de objetos do S3 concluídos em um determinado período de tempo. Dimensões válidas: • `Malware Protection Plan Id` `Resource Name` Unidades: contagem
`FailedScanCount`	O número de verificações de malware de objetos do S3 que falharam em um determina do período de tempo. Dimensões válidas: • `Malware Protection Plan Id` `Resource Name` Unidades: contagem

`SkippedScanCount`	O número de verificações de malware de objetos do S3 que foram ignorados em um determinado período de tempo.
	
	Dimensões válidas:
	
	• `Malware Protection Plan Id`
	
	`Resource Name`
	
	`Skipped Reason`
	
	Valores potenciais
	
	• `Unsupported`
	• `MissingPermissions`
	
	Unidades: contagem

Métricas de resultados da verificação de malware	
`InfectedScanCount`	O número de verificações de malware de objetos do S3 que detectaram objetos potencial mente maliciosos em um determinado período de tempo. Dimensões válidas: • `Malware Protection Plan Id` `Resource Name` Unidades: contagem

`CompletedScanBytes`	O número de bytes de objetos do S3 verificados em um determinado período de tempo. Dimensões válidas: • `Malware Protection Plan Id` `Resource Name` Unidades: contagem

> **Note**
>
> Por padrão, as estatísticas nas CloudWatch métricas são AVG.

As seguintes dimensões são suportadas para a Proteção contra Malware para métrica S3.

Dimensão	Descrição
`Malware Protection Plan Id`	O identificador exclusivo associado ao recurso do plano de Proteção contra Malware GuardDuty criado para seu recurso protegido.
`Resource Name`	O nome do recurso protegido.
`Skipped Reason`	O motivo pelo qual uma verificação de malware de objetos do S3 foi ignorada. Valores potenciais • `Unsupported` • `MissingPermissions`

Para obter informações sobre como acessar e consultar essas métricas, consulte Usar CloudWatch métricas da Amazon no Guia do CloudWatch usuário da Amazon.

Para obter informações sobre a configuração de alarmes, consulte Usando CloudWatch alarmes da Amazon no Guia CloudWatch do usuário da Amazon.

Solução de problemas

Conteúdo

- Solução de problemas do status do plano de proteção contra malware
- Solução de problemas de escaneamento de malware sob demanda

Solução de problemas do status do plano de proteção contra malware

Para qualquer bucket protegido, GuardDuty exibe o Status com base na classificação. Por exemplo, se um bucket protegido tiver problemas nas categorias Erro e Aviso, primeiro GuardDuty exibirá o problema associado ao status de Erro.

A lista a seguir inclui os erros e o aviso sobre o status do plano de Proteção contra Malware.

Erros

- EventBridge a notificação está desativada para este bucket S3
- EventBridge A regra gerenciada para receber eventos de bucket do S3 está ausente
- bucket do S3 não existe mais

Aviso

Não foi possível colocar o objeto de teste

EventBridge a notificação está desativada para este bucket S3

O código do motivo do status associado é`EVENTBRIDGE_MANAGED_EVENTS_DELIVERY_DISABLED`.

Detalhe do status

GuardDuty usa EventBridge para receber uma notificação quando um novo objeto é carregado nesse bucket do S3. Essa permissão está ausente em seu perfil do IAM.

Etapas para solucionar problemas

Opção 1: adicione a seguinte declaração de permissão ao seu perfil do IAM:

```
{
          "Sid": "AllowEnableS3EventBridgeEvents",
          "Effect": "Allow",
          "Action": [
             "s3:PutBucketNotification",
             "s3:GetBucketNotification"
             ],
          "Resource": [
             "arn:aws:s3:::amzn-s3-demo-bucket"
            ]
}
```

Substitua *amzn-s3-demo-bucket* pelo nome do bucket do Amazon S3.

Opção 2: ativar a EventBridge notificação usando o console do Amazon S3

1. Abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. Na página Buckets, na guia Buckets de uso geral, selecione o nome do bucket associado a esse erro.
3. Na página do bucket, escolha a aba Propriedades.
4. Na EventBridge seção Amazon, selecione Editar.
5. Na EventBridge página Editar Amazon, em Enviar notificação à Amazon EventBridge para todos os eventos neste bucket, selecione Ativado.
6. Escolha Salvar alterações.

Pode levar alguns minutos para que o valor da coluna Status mude para Ativo.

EventBridge A regra gerenciada para receber eventos de bucket do S3 está ausente

O código do motivo do status associado é`EVENTBRIDGE_MANAGED_RULE_DISABLED`.

Detalhe do status

As permissões da regra EventBridge gerenciada para gerenciar a configuração da EventBridge regra estão ausentes.

Etapas para solucionar problemas

Adicione a seguinte declaração de permissão ao seu perfil do IAM:

```
{
         "Sid": "AllowManagedRuleToSendS3EventsToGuardDuty",
        "Effect": "Allow",
        "Action": [
               "events:PutRule",
               "events:DeleteRule",
               "events:PutTargets",
               "events:RemoveTargets"
            ],
        "Resource": [
           "arn:aws:events:*:*:rule/DO-NOT-DELETE-
AmazonGuardDutyMalwareProtectionS3*"
           ],
        "Condition": {
           "StringEquals": {
              "events:ManagedBy": "malware-protection-plan.guardduty.amazonaws.com"
              }
           }
}
```

Pode levar alguns minutos para que o valor da coluna Status mude para Ativo.

bucket do S3 não existe mais

O código do motivo do status associado é`PROTECTED_RESOURCE_DELETED`.

Detalhe do status

Esse bucket do S3 foi excluído da sua conta e não existe mais.

Etapas para solucionar problemas

Se a exclusão do bucket do S3 não foi intencional, você pode criar um novo bucket usando o console do Amazon S3.

Depois de criar o bucket com sucesso, ative a Proteção contra malware para S3 seguindo as etapas abaixo da página Configurando a proteção contra malware para S3 para seu bucket.

Não foi possível colocar o objeto de teste

O código do motivo do status associado é`INSUFFICIENT_TEST_OBJECT_PERMISSIONS`.

> **Note**
>
> A permissão para adicionar um objeto de teste é opcional. A falta dessa permissão em seu perfil do IAM não impede que a Proteção contra Malware para S3 inicie a verificação de malware em um objeto recém-carregado. Depois que uma verificação for iniciada com sucesso, pode levar alguns minutos para que o status do plano de proteção contra malware mude de Aviso para Ativo.
> Se o perfil do IAM já incluir essa permissão, esse aviso indica uma política restritiva de bucket do Amazon S3 que não permite que o IAM tenha acesso para colocar o objeto de teste nesse bucket do S3.

Detalhe do status

Para validar a configuração do bucket selecionado, GuardDuty coloca um objeto de teste em seu bucket.

Etapas para solucionar problemas

Você pode optar por atualizar o perfil do IAM para incluir as permissões ausentes. À função do IAM selecionada, adicione as seguintes permissões para que GuardDuty você possa colocar o objeto de teste no recurso selecionado:

```
{
        "Sid": "AllowPutValidationObject",
        "Effect": "Allow",
        "Action": [
          "s3:PutObject"
          ],
        "Resource": [
          "arn:aws:s3:::amzn-s3-demo-bucket/malware-protection-resource-validation-
object"
          ]
}
```

Substitua *amzn-s3-demo-bucket* pelo nome do bucket do Amazon S3. Para obter mais informações sobre permissões do perfil do IAM, consulte Criar ou atualizar a política do perfil do IAM.

Pode levar alguns minutos para que o valor da coluna Status mude para Ativo.

Solução de problemas de escaneamento de malware sob demanda

Não foi possível iniciar um escaneamento.

Certifique-se de que a solicitação de verificação contenha uma entrada válida e que o Plano de Proteção contra Malware esteja ativado para o bucket.

Editando o plano de proteção contra malware para um bucket protegido

Talvez seja necessário editar a política de permissões preferencial do IAM, ativar ou desativar a marcação do objeto S3 verificado ou adicionar ou remover prefixos de objetos do S3. Por exemplo, ao ativar a Proteção contra malware para S3 para seu bucket, você decidiu não habilitar a marcação do objeto S3 verificado com o resultado da verificação. No entanto, agora você deseja GuardDuty adicionar a tag predefinida e o resultado da verificação como o valor da tag.

Escolha um método de acesso preferencial para atualizar o plano de Proteção contra malware para S3 em seu bucket protegido do S3.

Console

Para editar um plano de proteção contra malware

1. Faça login no Console de gerenciamento da AWS e abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.
2. No painel de navegação, escolha Proteção contra Malware para S3
3. Em Buckets protegidos, selecione o bucket para o qual você deseja editar a configuração existente.
4. Escolha Editar.
5. Atualize a configuração existente e a definição do seu bucket e confirme as alterações. Para obter informações sobre a descrição e as etapas de cada seção, consulte Habilitando a proteção contra malware para S3 para seu bucket.

   Monitore a coluna Status desse bucket protegido. Se aparecer como Aviso ou Erro, consulteSolução de problemas do status do plano de proteção contra malware.

API/CLI

Para editar o plano de proteção contra malware usando a API ou AWS CLI

- Usando a API

  Execute a UpdateMalwareProtectionPlanAPI usando o ID do plano de Proteção contra Malware associado a esse recurso do plano.

  Para recuperar o ID do plano de proteção contra malware em uma região específica, você pode executar a ListMalwareProtectionPlansAPI nessa região.
- Usando AWS CLI

  A lista a seguir fornece AWS CLI exemplos de comandos para atualizar o recurso do plano de Proteção contra Malware. Você precisará do ID do plano de proteção contra malware associado ao seu bucket do S3.

  AWS CLI exemplos de comandos

  - Use o AWS CLI comando a seguir para ativar ou desativar a marcação do recurso do plano de proteção contra malware associado ao seu bucket do S3:

    ```
    aws guardduty update-malware-protection-plan --malware-protection-plan-
    id 4cc8bf26c4d75EXAMPLE --actions "Tagging"={"Status"="ENABLED|DISABLED"}
    ```
  - Use o AWS CLI comando a seguir para adicionar um prefixo de objeto ao recurso do plano de proteção contra malware associado ao seu bucket do S3:

    ```
    aws guardduty update-malware-protection-plan --malware-
    protection-plan-id 4cc8bf26c4d75EXAMPLE --protected-resource
     "S3Bucket"={"ObjectPrefixes"=["amzn-s3-demo-1", "amzn-s3-demo-2"]}
    ```

    Certifique-se de incluir os prefixos de objeto existentes nesse comando; caso contrário, GuardDuty removerá esses prefixos ao editar o recurso do plano de Proteção contra Malware.
  - Use o AWS CLI comando a seguir para remover um prefixo de objeto do recurso do plano de proteção contra malware associado ao seu bucket do S3:

    ```
    aws guardduty update-malware-protection-plan --malware-protection-plan-
    id 4cc8bf26c4d75EXAMPLE --protected-resource "S3Bucket"={"ObjectPrefixes"=[""]}
    ```

Se você ainda não tiver o ID do plano de proteção contra malware para esse recurso, execute o AWS CLI comando a seguir e *us-east-1* substitua-o pela região para a qual deseja listar os IDs do plano de proteção contra malware.

```
aws guardduty list-malware-protection-plans --region us-east-1
```

Desativando a proteção contra malware para S3 em um bucket protegido

Quando você desativa a Proteção contra Malware para S3 em um bucket protegido, GuardDuty exclui o ID do plano de Proteção contra Malware associado a esse bucket. GuardDuty não iniciará mais uma verificação de malware quando um novo objeto for carregado nesse bucket ou em um dos prefixos de objeto selecionados.

Se você ativou GuardDuty e agora deseja suspender ou desativar GuardDuty, consulteSuspensão ou desativação GuardDuty. Como não há conceito de ID de detector no Malware Protection for S3, desabilitar ou suspender GuardDuty não afeta o status de um bucket protegido em sua conta. Você pode continuar usando o recurso Proteção contra Malware para S3 independentemente do preço padrão associado. Para obter mais informações, consulte Analisando o custo de uso da Proteção contra Malware para S3. Para parar de usar a Proteção contra Malware para S3, você precisará desativá-la para todos os buckets protegidos em sua conta. Se você quiser continuar usando GuardDuty e desabilitar somente o Malware Protection for S3 para um bucket, as etapas a seguir não afetarão a configuração do GuardDuty serviço e de outros planos de proteção que você possa ter ativado.

Escolha um método de acesso preferencial para desativar a Proteção contra malware para S3 em seu bucket protegido do S3.

Console

Para desativar a Proteção contra Malware para S3 usando o console GuardDuty

1. Faça login no Console de gerenciamento da AWS e abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.
2. No painel de navegação, escolha Proteção contra Malware para S3.

3. Em Buckets protegidos, selecione o bucket para o qual você deseja desativar a Proteção contra Malware para S3.

   Você pode selecionar somente um bucket protegido por vez. Para desativar a Proteção contra Malware para S3 para mais de um bucket, siga estas etapas novamente para outro bucket S3.

4. Escolha Desativar para confirmar a seleção.

API/CLI

Para desativar a Proteção contra Malware para S3 usando a API ou AWS CLI

- Usando a API

  Execute a DeleteMalwareProtectionPlanAPI usando o ID do plano de Proteção contra Malware associado a esse recurso do plano.

  Para recuperar o ID do plano de Proteção contra Malware, você pode executar a ListMalwareProtectionPlansAPI.

- Usando AWS CLI

  Como alternativa, você pode executar o AWS CLI comando a seguir para desativar a Proteção contra Malware para S3 *4cc8bf26c4d75EXAMPLE* substituindo-a pela ID do plano de Proteção contra Malware associada a esse bucket do S3:

  ```
  aws guardduty delete-malware-protection-plan --malware-protection-plan-
  id 4cc8bf26c4d75EXAMPLE
  ```

  Se você ainda não tiver o ID do plano de proteção contra malware para esse bucket do S3, execute o AWS CLI comando a seguir e *us-east-1* substitua-o pela região para a qual deseja listar os IDs do plano de proteção contra malware.

  ```
  aws guardduty list-malware-protection-plans --region us-east-1
  ```

Suportabilidade dos atributos do Amazon S3

A tabela a seguir especifica se a Proteção contra Malware para S3 é compatível ou não com os atributos listados do Amazon S3.

É disponibilizado suporte?	Description
Sim	Os objetos do S3 podem ser recuperados sem restauração assíncrona.

É disponibilizado suporte?	Description
Condicional	• O suporte ao Intelligent Tiering está disponível para objetos do S3 nos níveis Frequent, Infrequent e Archive Instance Access. • Os níveis opcionais Archive e Deep Archive não são suportadas. • O Intelligent Tiering sempre cria um novo objeto no nível de Acesso Frequente. Portanto, a verificação de objetos na criação é suportada. • Atributos futuros de Intelligent tiering podem criar objetos no Archive. Portanto, isso não é suportado.

É disponibilizado suporte?	Description
Não	GuardDuty suporta somente buckets de uso geral para o Malware Protection for S3.

É disponibilizado suporte?	Description
Não	Os objetos do S3 devem ser restaurados antes de serem acessados.
Não	Proteção contra Malware para S3 não é compatível com Outposts.

É disponibilizado suporte?	Description
Sim	Todos os objetos do S3 enviados são verificados em busca de malware. Se você fez upload de um objeto com a versão v1 do arquivo e imediatamente fez o upload de outra versão substituída pela v2, GuardDuty digitaliz ará as versões v1 e v2 do arquivo objeto. No entanto, o horário de início da verificação pode não estar na mesma ordem.
Sim	Se o bucket de destino for um recurso protegido, ele GuardDuty examinará todos os objetos do S3 que são replicados para os prefixos protegidos e monitorados.
Não	Você não pode definir uma regra de replicação com base na tag do resultado da verificação. O Amazon S3 não oferece suporte à replicação de tags, exceto na criação.

É disponibilizado suporte?	Description
Sim	GuardDuty suporta escaneamentos de malware para objetos do S3 que são criptografados com chaves gerenciadas e gerenciadas pelo cliente. Certifique-se de que o perfil do IAM inclua a permissão para usar a chave. Para obter mais informações, consulte Adicionar permissões de política do IAM.

É disponibilizado suporte?	Description
Não	A Proteção contra Malware para S3 não oferece suporte à verificação de objetos do S3 criptografados com chaves que não estão acessíveis.
Não	Quando os objetos do Amazon S3 são criptografados usando o Cliente de criptografia do Amazon S3, eles não são expostos a terceiros, incluindo a AWS. Para obter mais informações sobre por que isso não é compatível, consulte Proteção de dados usando criptografia do lado do cliente. **Note** CSE-KMS objetos criptografados são recebidos como um blob criptografado em que a criptografia não pode ser determinada. Portanto, GuardDuty processa-os à medida que são recebidos e verifica o blob criptografado como um arquivo normal. GuardDuty não retorna um status de `UNSUPPORTED` digitalização para esses objetos, a menos que algum deles Quotas na Proteção contra malware para o S3 exceda.

É disponibilizado suporte?	Description
Sim	Objetos S3 bloqueados são bloqueados com base em WORM - Write Once Read Many. A Proteção contra Malware para S3 pode acessar e verificar os objetos.
Sim	A Proteção contra Malware para S3 pode verificar os buckets configurados com o Requester Pays. O solicitante pagará pelas chamadas do S3. Para obter mais informações, consulte Configuração de buckets de Pagamento pelo solicitante para transferências de armazenamento e uso no Guia do usuário do Amazon S3.
Sim	Você pode definir políticas de ciclo de vida com base na tag de resultado da verificação. Por exemplo, exclua automaticamente objetos maliciosos. Para obter mais informações sobre configurações do ciclo de vida, consulte Gerenciar o ciclo de vida do armazenamento no Guia do usuário do Amazon S3.

É disponibilizado suporte?	Description
Sim	Você pode definir políticas de recursos de bucket com base na sua tag de resultado de verificação de objetos do S3. Por exemplo, impeça o acesso a objetos do S3 que ainda não foram escaneados ou a ameaças GuardDuty detectadas. Para obter mais informações, consulte Usando controle de acesso baseado em tags (TBAC) com proteção contra malware para S3.
Não	O Malware Protection for S3 verifica somente o conteúdo do objeto do S3.

Quotas na Proteção contra malware para o S3

Esta seção fornece as quotas predefinidas, referidas frequentemente como limites. A menos que especificado, cada cota é Region-specific. Para ver as cotas padrão específicas para o uso do GuardDuty serviço básico, consulte. GuardDuty Cotas da Amazon

As tabelas a seguir descrevem as várias cotas que se aplicarão à sua Conta da AWS.

AWS valor da cota padrão	É ajustável?	Description
100 GB	Não	O tamanho máximo do objeto do S3 que GuardDuty tentará verificar se há malware.

AWS valor da cota padrão	É ajustável?	Description
100.000	Não	O número máximo de arquivos que GuardDuty podem ser extraídos e analisados em um objeto do S3. **Note** Os tipos de arquivos compostos estão potencialmente sujeitos a esses limites. Os tipos de arquivo incluem, mas não estão limitados a, mensagens de e-mail codificadas em MIME (Multipurpose Internet Mail Extensions), arquivos Python (PYC) compilados, arquivos de ajuda HTML compilada (CHM), todos os instaladores e documentos em formato (ODF). OpenDocument **Note** Objetos do S3 com uma taxa de compressão extremamente alta entre o tamanho do objeto do S3 e o tamanho do conteúdo extraído podem estar sujeitos a limites, mesmo que os arquivos extraídos estejam abaixo dessa cota.

AWS valor da cota padrão	É ajustável?	Description
100	Não	Os níveis máximos de aninhamento que GuardDuty podem ser extraídos em um objeto do S3.
25	Não	O número máximo de buckets do S3 para os quais você pode ativar a Proteção contra malware para o S3. Esse limite de cota é por conta em cada região.

GuardDuty Proteção contra malware para AWS Backup

Tópicos

- Visão geral do
- Como funciona a Proteção contra Malware para Backup?
- GuardDuty Proteção contra malware para backup: permissões de função do IAM
- (Opcional) Comece a usar o Malware Protection for Backup Independently (somente console)
- Iniciando uma On-Demand verificação de proteção contra malware para backup
- Monitoramento de status e resultados de escaneamento no Malware Protection for Backup
- Cotas de proteção contra malware para backup

Visão geral do

O Malware Protection for Backup ajuda você a detectar a possível presença de malware em seus dados de backup examinando recursos AWS protegidos por backup, como snapshots do Amazon EBS, AMIs do Amazon EC2 e pontos de recuperação do Amazon S3. Quando o AWS Backup cria ou atualiza um recurso de backup protegido, GuardDuty pode executar uma verificação de malware nesse backup para ajudar a identificar conteúdo potencialmente malicioso antes que ele seja restaurado em seu ambiente.

Como você pode usar a Proteção contra Malware para Backup

Você pode usar esse recurso em dois modos, dependendo se GuardDuty está habilitado em sua conta:

1. Usando a Proteção contra Malware para Backup com a GuardDuty opção ativada

   Quando GuardDuty ativado em uma região, o AWS Backup integra a Proteção contra Malware ao fluxo de trabalho de GuardDuty descobertas. Os resultados da verificação de malware aparecem nas GuardDuty descobertas, além da Amazon EventBridge e da Amazon CloudWatch.
2. Usando a Proteção contra Malware para Backup sem habilitar GuardDuty

   Você pode usar o Malware Protection for Backup de forma independente, sem ativar o GuardDuty serviço completo. Nesse modo, os resultados da verificação permanecem totalmente disponíveis por meio de EventBridge CloudWatch e.

Considerações sobre o uso independente do Malware Protection for Backup

Ao usar o recurso sem habilitar GuardDuty:

- A configuração do plano de backup é gerenciada inteiramente no AWS Backup.

GuardDuty não fornece controles para selecionar planos de backup, cofres ou tipos de recursos. Todas as habilitações, agendamentos e configurações de políticas permanecem no Backup. AWS

- GuardDuty as descobertas não são geradas.

As descobertas exigem uma ID de detector, que é criada somente quando GuardDuty ativada. Ao usar a Proteção contra Malware de forma independente, os resultados da verificação são exibidos exclusivamente por meio de EventBridge eventos e CloudWatch métricas.

- Você ainda pode iniciar escaneamentos sob demanda a partir do console. GuardDuty

Mesmo quando não GuardDuty está habilitado, o GuardDuty console fornece um fluxo de trabalho para iniciar uma verificação de malware sob demanda em busca de tipos de recursos de backup compatíveis. Isso permite que os clientes usem uma GuardDuty interface familiar sem precisar do GuardDuty serviço completo.

- Non-GuardDuty os clientes podem acessar os fluxos de trabalho de iniciação de escaneamento.

Os pontos de entrada do escaneamento sob demanda estão disponíveis para todos os clientes que usam o Malware Protection for Backup, independentemente da existência de um GuardDuty detector na conta.

- O comportamento e a cobertura do escaneamento permanecem idênticos.

Ativado ou não, o recurso verifica os mesmos tipos de recursos de AWS Backup com o mesmo mecanismo de detecção de malware. GuardDuty A única diferença é onde os resultados são publicados.

Esse modelo permite que os clientes adotem a verificação de malware para backups sem a necessidade GuardDuty de recursos mais amplos de detecção de ameaças, ao mesmo tempo em

que fornece um GuardDuty-based fluxo de trabalho opcional para iniciar e visualizar as operações de verificação.

Como funciona a Proteção contra Malware para Backup

O Malware Protection for Backup pode verificar os seguintes AWS recursos protegidos por backup:

- Snapshots do Amazon EBS
- AMIs do Amazon EC2
- Pontos de recuperação do Amazon S3 e backups contínuos do S3 ou recuperação pontual (PITR)
- Cofres bloqueados (imutáveis) (pontos de EBS/EC2 recuperação) usando o AWS Backup Vault Lock em regiões suportadas

Digitalização incremental

AWS O Backup captura alterações incrementais em vários tipos de recursos. GuardDuty tem a capacidade de escanear somente os blocos ou objetos novos ou alterados quando um backup é criado ou atualizado, melhorando o desempenho e reduzindo a sobrecarga de digitalização, ao mesmo tempo em que obtém cobertura total ao longo do tempo.

On-demand escaneamento

Você pode iniciar um escaneamento em qualquer recurso de backup compatível a qualquer momento, diretamente do AWS Backup ou do console. GuardDuty Os casos de uso comuns incluem verificar um backup antes da restauração, verificar novamente dados antigos após a publicação de novas assinaturas de ameaças ou realizar verificações periódicas de conformidade.

> **Note**
>
> - A Proteção contra Malware para Backup só pode ser ativada para recursos de backup na mesma região.
> - GuardDuty digitaliza uma cópia somente para leitura do backup; ela não modifica o conteúdo do backup.
> - A digitalização funciona tanto para cofres padrão quanto para cofres bloqueados (imutáveis).

Como funciona a Proteção contra Malware para Backup?

Esta seção descreve os componentes do Malware Protection for Backup, como ele funciona e como você pode analisar o status e o resultado da verificação de malware.

Visão geral do

A Proteção contra Malware para Backup é um recurso que ajuda a detectar a presença de malware em instantâneos do EBS, imagens EC2 (AMI) e pontos de recuperação pertencentes aos tipos de recursos EBS, EC2 e S3. Você pode iniciar uma verificação de malware sob demanda por meio do GuardDuty console ou da API transmitindo uma função do IAM que fornece as permissões necessárias para a verificação, junto com um ou dois ARNs de recursos, dependendo da categoria de verificação. Há duas categorias de escaneamento possíveis: escaneamentos completos e escaneamentos incrementais.

Verificação completa e verificação incremental

Uma verificação completa é quando a API aceita o ARN de um recurso e verifica todos os arquivos dentro desse recurso. Por outro lado, uma varredura incremental usa dois ARNs de recursos, ambos pertencentes ao mesmo recurso, e verifica os arquivos alterados entre eles. Como exemplo, vamos supor que tiramos um instantâneo de um volume do EBS. Vamos chamá-lo de snapshot-1. Se uma verificação completa for feita nesse instantâneo, GuardDuty verificará todos os arquivos contidos nesse instantâneo. Agora, vamos supor que alguns arquivos foram adicionados ao mesmo volume e um novo instantâneo foi tirado. Vamos chamá-lo de snapshot-2. Como apenas alguns arquivos foram alterados entre snapshot-1 e snapshot-2, pode-se acionar uma verificação incremental com os ARNs de recursos desses dois instantâneos. Nesse caso, snapshot-2 é chamado de `target` recurso e snapshot-1 é chamado de recurso. `base` Você verá essa terminologia usada no restante do documento. Essa verificação incremental examinará os arquivos alterados entre snapshot-1 e snapshot-2.

Análise de malware para Point-in-Time-Recovery (PITR)

Quando ativada a partir do AWS Backup, a verificação de malware para backups contínuos ou PITR ocorre de acordo com a frequência configurada no plano de Backup. Isso é orquestrado pelo serviço de AWS Backup. Por exemplo, GuardDuty executará a primeira varredura de t0 a t2, a próxima varredura de t2 a t4, a varredura subsequente de t4 a t6 e assim por diante. Cada um desses escaneamentos gera um ID de escaneamento que pode ser consultado usando a `GetMalwareScan` API para obter o status e o resultado do escaneamento nesse período.

Como alternativa, você também pode escanear todo o recurso PITR a partir do GuardDuty console ou usando a GuardDuty `StartMalwareScan` API sob demanda, passando um carimbo de data e hora de término. Isso garantirá que GuardDuty escaneie todo o recurso desde o início até o registro de data e hora final.

> **Note**
>
> - Você não pode acionar varreduras parciais ou incrementais no PITR a partir de. GuardDuty
> - O carimbo de data/hora final passado para uma varredura sob demanda não pode ser anterior a (hora atual - 15 minutos).

Examinando novamente arquivos infectados anteriormente em uma verificação incremental

Como parte de uma verificação incremental, também GuardDuty examinará novamente os arquivos infectados anteriormente a partir da verificação básica por até 365 dias.

Requisitos para uma verificação incremental

Os requisitos a seguir devem ser atendidos GuardDuty para realizar uma varredura incremental. Se algum desses requisitos não for atendido, GuardDuty pulará a verificação.

- O recurso básico deve ser escaneado nos últimos 365 dias e o resultado da verificação deve estar em `COMPLETED` ou`COMPLETED_WITH_ISSUES`.
- O recurso base deve ter uma data de criação anterior à do recurso de destino.
- Os recursos base e de destino devem ter o mesmo tipo de criptografia no caso de instantâneos.
- Os recursos base e alvo devem ser da mesma linhagem.
  - Para um snapshot do EBS e um ponto de recuperação do EBS, isso significa que eles vêm do mesmo volume ou são cópias do mesmo volume, sem nenhuma alteração no tipo de criptografia.
  - Para um ponto de recuperação do S3, os ARNs dos recursos base e de destino devem ser criados a partir do mesmo bucket S3 subjacente.
  - No caso de AMIs, pares de instantâneos são comparados entre a AMI base e a de destino para identificar instantâneos para uma verificação incremental. Cada par de instantâneos precisa

atender às condições mencionadas acima. Qualquer instantâneo dentro da AMI de destino que não tenha um instantâneo correspondente na AMI base será ignorado.

Re-scanning Recursos de backup digitalizados anteriormente

Você pode iniciar uma nova verificação de malware sob demanda no mesmo recurso após 10 minutos a partir da hora de início da verificação de malware anterior. Se a nova verificação de malware for iniciada dentro de 10 minutos após o início da verificação de malware anterior, sua solicitação resultará no seguinte erro e nenhuma ID de verificação será gerada para essa solicitação. As etapas para verificar novamente a instância permanecem as mesmas usadas para iniciar uma verificação de malware sob demanda pela primeira vez.

Função do IAM necessária para digitalização

Você precisa passar uma função do IAM para iniciar uma verificação completa ou incremental. Essa função fornece as permissões necessárias para realizar as operações de varredura. GuardDuty Proteção contra malware para backup: permissões de função do IAMfornece a lista exata das permissões necessárias, junto com a política de confiança relevante necessária para realizar a verificação.

Analisando o status e o resultado do escaneamento de recursos

GuardDuty publica o evento do resultado da digitalização no barramento de eventos EventBridge padrão da Amazon. GuardDuty usa entrega pelo menos uma vez, o que significa que você pode receber vários resultados de escaneamento para o mesmo objeto. Recomendamos projetar suas aplicações para lidar com resultados duplicados. Você é cobrado apenas uma vez por cada objeto verificado.

Para obter mais informações, consulte Monitoramento de status e resultados de escaneamento no Malware Protection for Backup.

Revisar descobertas geradas

A análise das descobertas depende de você estar ou não usando o Malware Protection for Backup com GuardDuty. Considere os seguintes cenários:

Usando a Proteção contra Malware para Backup quando o GuardDuty serviço está ativado (ID do detector)

Se a verificação de malware detectar um arquivo potencialmente malicioso em um recurso de Backup escaneado, GuardDuty gerará uma descoberta associada. É possível visualizar os detalhes da descoberta e usar as etapas recomendadas para corrigir a descoberta. Com base na frequência de suas descobertas de exportação, a descoberta gerada é exportada para um bucket do S3 e para um barramento de EventBridge eventos da Amazon.

Para obter informações sobre o tipo de descoberta que seria gerado, consulte Proteção contra malware para tipos de descoberta de Backup Como encontrar tipos de proteção contra malware para backup.

Usando a Proteção contra Malware para Backup como um recurso independente (sem ID de detector)

GuardDuty não será capaz de gerar descobertas porque não há uma ID de detector associada. Para saber o status do escaneamento do seu recurso de backup, você pode ver o resultado do escaneamento que é publicado GuardDuty automaticamente no seu barramento de eventos padrão.

Para obter informações sobre o status e o resultado da verificação, consulteMonitoramento de status e resultados de escaneamento no Malware Protection for Backup.

> **Note**
>
> Se você também estiver usando o Malware Protection for S3, é possível que seu arquivo S3 tenha sido marcado anteriormente como NO_THREATS_FOUND e, ainda assim, o mesmo arquivo possa aparecer na lista de ameaças do Backup Recovery Point ao qual o objeto pertence. Isso acontece porque o serviço atualiza frequentemente suas assinaturas de malware, o que pode ter alterado o status do arquivo. Observe que, nesses casos, GuardDuty não volta e atualiza a tag no arquivo no bucket S3 original. A única maneira de aplicar uma tag atualizada ao arquivo é recarregando o objeto no bucket ou usando o recurso de varredura sob demanda do S3.

GuardDuty Proteção contra malware para backup: permissões de função do IAM

Função de cliente fornecida para verificação de malware

GuardDuty A Proteção contra Malware espera que uma função de cliente (função de scanner) seja fornecida quando as verificações são iniciadas nos recursos de Backup, ou seja, instantâneos, AMIs

e EBS/EC2/S3 pontos de recuperação. Essa função fornece as permissões necessárias GuardDuty para realizar a verificação nesses recursos específicos. A política de permissões e a política de confiança para essa função podem ser encontradas emPolítica de permissões e confiança para a função. A seção abaixo descreve por que cada uma dessas permissões é necessária.

Detalhes sobre as permissões

- `ModifySnapshotAttribute`- Permite que instantâneos criptografados com chave não criptografada e gerenciados pelo cliente sejam acessados pela conta de serviço do GuardDuty Malware Protection.
- `CreateGrant`- Permite que a Proteção contra GuardDuty Malware crie e acesse um volume EBS criptografado com chave gerenciada pelo cliente a partir do instantâneo criptografado da chave gerenciada pelo cliente ao qual a conta de GuardDuty serviço tem acesso.
- `RetireGrant`- Permite que a Proteção contra GuardDuty Malware retire as concessões criadas na Chave Gerenciada pelo Cliente para leitura de instantâneos criptografados
- `ReEncryptToe ReEncryptFrom` - Exigido pelo EBS para dar GuardDuty acesso a instantâneos criptografados com chaves gerenciadas pelo cliente e criar volumes criptografados a partir delas. Embora os clientes possam considerar ReEncryption um instantâneo durante o compartilhamento como uma transição fundamental, os instantâneos permanecem imutáveis do ponto de vista do cliente depois de criados.
- `ListSnapshotBlockse GetSnapshotBlock` - As APIs do EBS Direct são usadas para acessar os blocos de instantâneos de um instantâneo criptografado com chave AWS gerenciada. Isso é feito porque os instantâneos criptografados com chave AWS gerenciada não podem ser acessados de outra forma entre contas.
- `Decrypt`- Permite descriptografar instantâneos básicos que são criptografados por chave gerenciada pelo cliente quando são baixados na memória usando as APIs do EBS Direct como parte da verificação incremental.
- `ListChangedBlocks`- API EBS Direct usada na verificação incremental de instantâneos para obter a lista de blocos alterados entre dois instantâneos.
- `DescribeKey`- Permite que a Proteção contra GuardDuty Malware determine o ID da chave AWS gerenciada na conta do cliente.
- `DescribeImages`- Permite que uma AMI seja descrita para obter a lista de instantâneos pertencentes à AMI.
- `DescribeRecoveryPoint`- Permite que o serviço busque os detalhes do ponto de recuperação e verifique o tipo de recurso do ponto de recuperação.

- `CreateBackupAccessPoint`,`DescribeBackupAccessPoint`, `DeleteBackupAccessPoint` - Permite que o serviço crie, descreva e exclua o ponto de acesso necessário para acessar os pontos de recuperação.
- `kms:Decrypt`- Permite que o serviço acesse objetos em um ponto de recuperação do S3 durante uma verificação do ponto de recuperação do S3.

Protegendo a função

A função deve ser configurada com uma política de confiança que confie no diretor do serviço de Proteção contra GuardDuty Malware. Isso garante que nenhum diretor além do GuardDuty serviço possa assumir essa função. Além disso, você é incentivado a reduzir as políticas a recursos específicos, em vez de*. Isso inclui IDs de instantâneos e IDs de chave. Isso garantirá que a função forneça acesso somente a esses recursos específicos.

> **Important**
>
> A configuração incorreta pode resultar em falhas de varredura devido a permissões insuficientes.

Como a Proteção contra GuardDuty Malware usa subsídios em AWS KMS

GuardDuty A Proteção contra Malware exige subsídios para usar suas chaves KMS.

Quando você inicia uma verificação em um instantâneo criptografado ou em uma AMI do EC2 que consiste em instantâneos criptografados, o GuardDuty Malware Protection cria concessões em seu nome enviando uma CreateGrantsolicitação ao KMS. AWS Essas concessões dão GuardDuty acesso a uma chave específica em sua conta.

GuardDuty A Proteção contra Malware exige a concessão para usar sua chave gerenciada pelo cliente para as seguintes operações internas:

- Envie DescribeKeysolicitações AWS para obter detalhes sobre a chave simétrica gerenciada pelo cliente com a qual o recurso enviado para uma verificação de malware está criptografado.
- Crie um volume do EBS a partir de um snapshot criptografado usando a CreateVolumeAPI e criptografe o volume com a mesma chave.
- Acesse blocos de instantâneos no instantâneo por meio da GetSnapshotBlockAPI durante uma verificação incremental.

- Envie solicitações de descriptografia ao AWS KMS para descriptografar as chaves de dados criptografadas para que elas possam ser usadas para ler os dados no instantâneo durante a verificação.

Você pode revogar a concessão criada ou remover o acesso do serviço à chave gerenciada pelo cliente a qualquer momento. Se você fizer isso, GuardDuty não conseguirá acessar nenhum dos dados criptografados pela chave gerenciada pelo cliente, o que afeta as operações que dependem desses dados.

GuardDuty Contexto de criptografia de proteção contra malware

Um contexto de criptografia é um conjunto opcional de pares de chave/valor que pode conter informações contextuais adicionais sobre os dados.

Quando você inclui um contexto de criptografia em uma solicitação para criptografar dados, o AWS KMS; vincula o contexto de criptografia aos dados criptografados. Para descriptografar os dados, você inclui o mesmo contexto de criptografia na solicitação.

GuardDuty A Proteção contra Malware usa um dos dois contextos de criptografia.

Contexto de criptografia 1: A chave é`aws:guardduty:id`.

```
"encryptionContext": {
    "aws:guardduty:id": "snap-11112222333344"
}
```

Esse contexto de criptografia é usado com operações de concessão: CreateGrant, Decrypt,,, GenerateDataKeyWithoutPlaintext, ReEncryptTo. RetireGrant DescribeKey

Uma concessão é criada no recurso atual com esse contexto de criptografia e operações de concessão.

Contexto de criptografia 2: A chave é `aws:ebs:id`

```
"encryptionContext": {
    "aws:ebs:id": "snap-11112222333344"
}
```

Esse contexto de criptografia é usado com operações de concessão: ReEncryptFrom, Decrypt,,. RetireGrant DescribeKey

Três concessões são criadas com esses contextos de criptografia e operações de concessão. Um no instantâneo de destino com a operação de `ReEncryptFrom` concessão. Um segundo no instantâneo de destino com `Decrypt, RetireGrant, DescribeKey` operações. E uma terceira no instantâneo básico com as mesmas operações de concessão da segunda concessão.

Política de permissões e confiança para a função

Política de permissões

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": [
                "ebs:ListSnapshotBlocks",
                "ebs:ListChangedBlocks",
                "ebs:GetSnapshotBlock"
            ],
            "Resource": "arn:aws:ec2:*::snapshot/*"
        },
        {
            "Sid": "CreateGrantPermissions",
            "Effect": "Allow",
            "Action": "kms:CreateGrant",
            "Resource": "arn:aws:kms:*:*:key/*",
            "Condition": {
                "ForAnyValue:StringLike": {
                    "kms:EncryptionContext:aws:guardduty:id": "snap-*",
                    "kms:ViaService": [
                        "guardduty.*.amazonaws.com",
                        "backup.*.amazonaws.com"
                    ]
                },
                "ForAllValues:StringEquals": {
                    "kms:GrantOperations": [
                        "Decrypt",
                        "CreateGrant",
                        "GenerateDataKeyWithoutPlaintext",
                        "ReEncryptFrom",
                        "ReEncryptTo",
                        "RetireGrant",
                        "DescribeKey"
                    ]
```

```
                },
                "Bool": {
                    "kms:GrantIsForAWSResource": "true"
                }
            }
        },
        {
            "Sid": "CreateGrantPermissionsForReEncryptAndDirectAPIs",
            "Effect": "Allow",
            "Action": "kms:CreateGrant",
            "Resource": "arn:aws:kms:*:*:key/*",
            "Condition": {
                "ForAnyValue:StringLike": {
                    "kms:EncryptionContext:aws:ebs:id": "snap-*",
                    "kms:ViaService": [
                        "guardduty.*.amazonaws.com",
                        "backup.*.amazonaws.com"
                    ]
                },
                "ForAllValues:StringEquals": {
                    "kms:GrantOperations": [
                        "Decrypt",
                        "ReEncryptTo",
                        "ReEncryptFrom",
                        "RetireGrant",
                        "DescribeKey"
                    ]
                },
                "Bool": {
                    "kms:GrantIsForAWSResource": "true"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeImages",
                "ec2:DescribeSnapshots"
            ],
            "Resource": "*"
        },
        {
            "Sid": "ShareSnapshotPermission",
            "Effect": "Allow",
```

```
            "Action": [
                "ec2:ModifySnapshotAttribute"
            ],
            "Resource": "arn:aws:ec2:*:*:snapshot/*"
        },
        {
            "Sid": "ShareSnapshotKMSPermission",
            "Effect": "Allow",
            "Action": [
                "kms:ReEncryptTo",
                "kms:ReEncryptFrom"
            ],
            "Resource": "arn:aws:kms:*:*:key/*",
            "Condition": {
                "StringLike": {
                    "kms:ViaService": "ec2.*.amazonaws.com"
                }
            }
        },
        {
            "Sid": "DescribeKeyPermission",
            "Effect": "Allow",
            "Action": "kms:DescribeKey",
            "Resource": "arn:aws:kms:*:*:key/*"
        },
        {
            "Sid": "DescribeRecoveryPointPermission",
            "Effect": "Allow",
            "Action": [
                "backup:DescribeRecoveryPoint"
            ],
            "Resource": "*"
        },
        {
            "Sid": "CreateBackupAccessPointPermissions",
            "Effect" : "Allow",
            "Action" : [
                "backup:CreateBackupAccessPoint"
            ],
            "Resource": "arn:aws:backup:*:*:recovery-point:*"
        },
        {
            "Sid": "ReadAndDeleteBackupAccessPointPermissions",
            "Effect" : "Allow",
```

```
            "Action" : [
                "backup:DescribeBackupAccessPoint",
                "backup:DeleteBackupAccessPoint"
            ],
            "Resource": "*"
        },
        {
            "Sid": "KMSKeyPermissionsForInstantAccess",
            "Effect": "Allow",
            "Action": [
                "kms:Decrypt"
            ],
            "Resource": "arn:aws:kms:*:*:key/*",
            "Condition": {
                "StringLike": {
                    "kms:ViaService": "backup.*.amazonaws.com"
                }
            }
        }
    ]
}
```

Política de confiança

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "malware-protection.guardduty.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

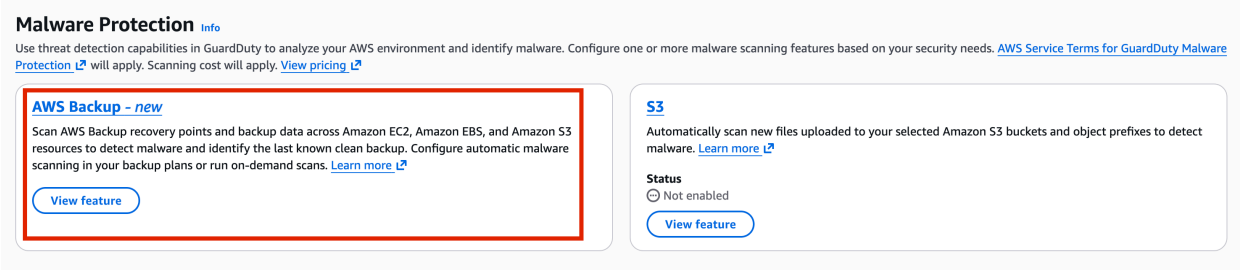
(Opcional) Comece a usar o Malware Protection for Backup Independently (somente console)

Use essa etapa opcional quando quiser começar a usar a opção de detecção de ameaças do Malware Protection for Backup, independente do GuardDuty status da sua AWS conta.

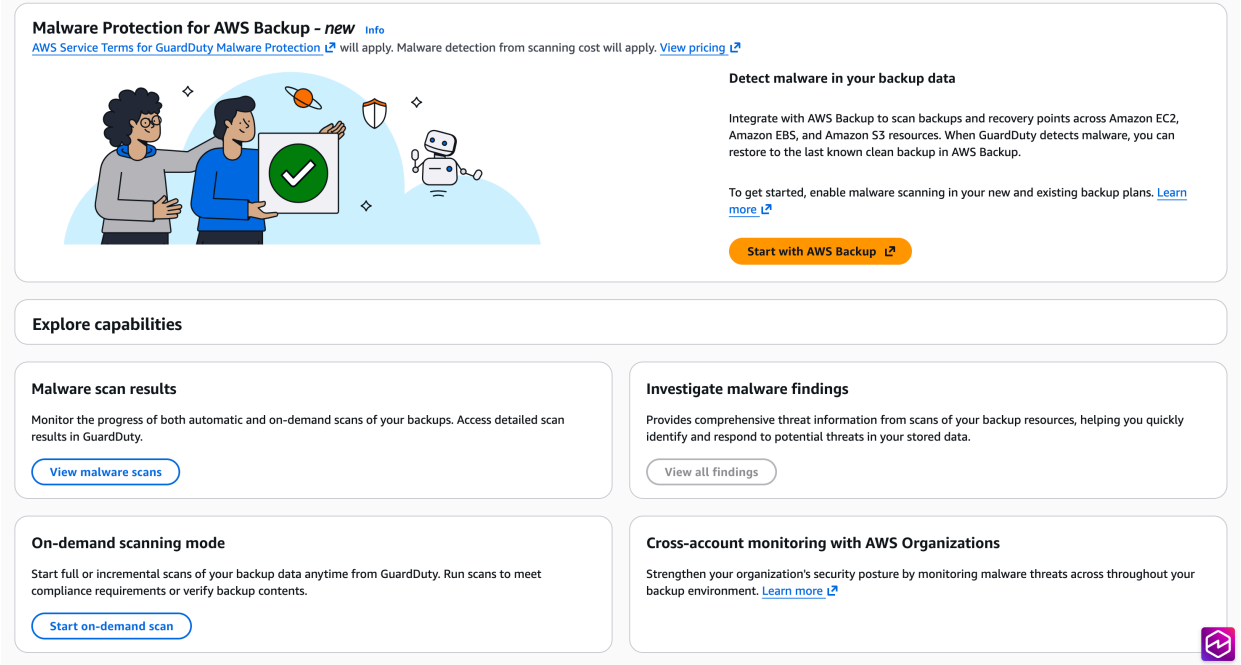
Se você também quiser usar outros planos de proteção dedicados GuardDuty, você deve começar a usar o GuardDuty serviço da Amazon. Para obter informações sobre planos de GuardDuty proteção, consulte Características do GuardDuty.

Etapas para começar a usar o Malware Protection for Backup

1. Faça login no AWS Management Console e abra o https://console.aws.amazon.com/guardduty/console em https://console.aws.amazon.com/guardduty/
2. Selecione Descubra os recursos de proteção contra malware e clique em Começar.
3. Ao clicar em Começar, você pode escolher entre as opções, incluindo os recursos de AWS Backup e Proteção contra Malware do S3.



4. Você é direcionado para a página Proteção contra Malware para Backup, onde pode escolher Iniciar uma verificação sob demanda ou Exibir escaneamentos de malware.



Iniciando uma On-Demand verificação de proteção contra malware para backup

Console

1. Faça login no AWS Management Console e abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.
2. Navegue até Malware Protection for Backup e clique em Iniciar escaneamento sob demanda.
3. Escolha entre escaneamento completo e escaneamento incremental.
    1. Para iniciar uma verificação completa, insira o ARN do recurso a ser verificado.
    2. Para uma verificação incremental, insira o ARN do recurso de destino e o ARN do recurso de linha de base.
    3. Se o recurso que está sendo escaneado for um Ponto de Recuperação, você também precisará inserir o nome do AWS Backup Vault ao qual ele pertence.
    4. Para um recurso PITR do S3, informe um carimbo de data e hora de término. O carimbo de data/hora de término não pode ser mais antigo do que (hora atual - 15 minutos).

4. Acesso ao serviço - você precisa escolher uma função que tenha as permissões necessárias para acessar o recurso e realizar a verificação. Clique em Exibir política para ver as permissões exatas necessárias para a função, juntamente com a política de confiança necessária.

Você pode fazer alterações na política com base em seus requisitos ou reduzir as permissões para o recurso exato. Para obter mais detalhes sobre como você pode criar ou atualizar uma função do IAM, consulteGuardDuty Proteção contra malware para backup: permissões de função do IAM.

Para problemas com permissões de função do IAM, consulte Solução de problemas de erro de permissões de função do IAM.

API/CLI

Invoke StartMalwareScanthat aceita o `resourceArn` recurso para o qual você deseja iniciar uma verificação de malware sob demanda. Se você quiser iniciar uma varredura incremental, passe a entrada`baselineResourceArn`. `incrementalScanDetails` Como parte da configuração do escaneamento, você também precisa fornecer uma função do IAM que tenha todas as permissões necessárias para iniciar o escaneamento. Se o recurso que está sendo escaneado for um recurso PITR do S3, você precisará passar um carimbo de data e hora de término. Depois de iniciar uma verificação com sucesso, `StartMalwareScan` retorna um `scanId`. Invoque a `GetMalwareScan` API para monitorar o progresso da verificação iniciada e obter detalhes da verificação depois de concluída.

Monitoramento de status e resultados de escaneamento no Malware Protection for Backup

Depois que uma verificação de malware é iniciada, GuardDuty fornece alguns mecanismos por meio dos quais você pode monitorar o status e o resultado de uma verificação. A tabela a seguir fornece alguns dos valores associados aos escaneamentos de malware.

Valores potenciais
`RUNNING`, `COMPLETED` , `COMPLETED_WITH_ISSUES` , `FAILED` ou `SKIPPED`

Valores potenciais
`FULL_SCAN` ou `INCREMENTAL_SCAN`
`GUARDDUTY_INITIATED` , `ON_DEMAND` ou `BACKUP_INITIATED`
`NO_THREATS_FOUND` ou `THREATS_FOUND`

*Observe que o status do resultado do escaneamento pode não estar presente se o escaneamento não tiver sido concluído. O status do resultado da verificação de THREATS_FOUND indica que foi GuardDuty detectada a presença de malware.

Para pontos de recuperação do S3, COMPLETED_WITH_ISSUES indica que alguns arquivos foram ignorados ou falharam. Para AMIs, COMPLETED_WITH_ISSUES indica que pelo menos 1 snapshot não pôde ser escaneado. Veja abaixo a lista de motivos ignorados.

As digitalizações também podem ser ignoradas por vários motivos. A tabela abaixo explica os motivos pelos quais os escaneamentos podem ser ignorados:

Motivo
A função do cliente não tem as permissões necessárias para que o serviço execute a verificação.
O recurso que está tentando ser escaneado não existe na conta ou foi excluído durante a verificação
O tamanho do instantâneo é maior do que o atualmente suportado pelo GuardDuty
Os recursos especificados na solicitação de verificação incremental não têm diferença
O recurso não está no estado esperado. Se a verificação for incremental, o ponto de recuperação básico não estará no estado DISPONÍVEL ou CONCLUÍDO
Para varreduras incrementais - os recursos base e atual não são da mesma linhagem
Para verificações incrementais - o recurso básico não foi escaneado anteriormente ou nenhuma verificação concluída foi encontrada

Motivo
Para varreduras incrementais - a data de criação do recurso base é maior que a data de criação do recurso atual
O tipo de recurso solicitado não oferece suporte à varredura incremental
AMIs públicas, AMIs com apenas armazenamento temporário e AMIs que não estão em um estado disponível não são elegíveis para verificação
Os instantâneos de armazenamento a frio não são elegíveis para digitalização
A digitalização não é suportada para tipos de recursos compostos
O recurso solicitado contém um código de produto do Amazon Marketplace que não é compatível com a digitalização

Motivo
As AMIs não suportam a digitalização de mais de 40 instantâneos
Nenhum mapeamento de dispositivo de bloco Ebs foi encontrado para o recurso solicitado
Para varreduras incrementais - o arn do recurso básico difere do arn do recurso esperado
Todos os arquivos na verificação foram ignorados ou falharam

Os resultados da verificação têm um período de retenção de 90 dias. Escolha seu método de acesso preferido para rastrear o status da verificação de malware.

Monitorando escaneamentos usando o console

1. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.
2. No painel de navegação, escolha Verificações de malware.

3. Você pode filtrar as verificações de malware pelas seguintes Propriedades disponíveis na barra de pesquisa de filtro.

   - ID do escaneamento — identificador exclusivo associado ao escaneamento de malware.
   - ID da conta — Conta em que a verificação de malware foi iniciada.
   - ARN do recurso — Nome do recurso da Amazon (ARN) associado ao recurso da Amazon associado ao escaneamento.
   - Tipo de recurso — O tipo de recurso associado à verificação, como Instância EC2, EBS Snapshot | EC2 AMI, EBS Recovery Point, EC2 Recovery Point ou S3 Recovery Point.
   - Status — O status do escaneamento, como Executando, Ignorado, Concluído, Concluído com Problemas ou Falha.
   - Tipo de escaneamento — Indica se foi um escaneamento de On-demand GuardDuty-initiated,, ou Backup-Initiated malware.

Monitorando escaneamentos usando o API/CLI

- Você pode invocar ListMalwareScans para filtrar escaneamentos de malware por `RESOURCE_ARNSCAN_ID`,`ACCOUNT_ID`,`SCAN_TYPE GUARDDUTY_FINDING_ID`,, `SCAN_STATUSRESOURCE_TYPE`, e. `SCAN_START_TIME` Você também pode invocar GetMalwareScan para recuperar metadados mais detalhados de um escaneamento fornecendo um ID de digitalização como entrada. Os critérios do `GUARDDUTY_FINDING_ID` filtro estão disponíveis quando o `SCAN_TYPE` é GuardDuty iniciado.
- Você pode alterar o exemplo *`filter-criteria`* no comando abaixo e filtrar com base `CriterionKey` em um de cada vez. As opções para `CriterionKey` são `Resource_ARNSCAN_ID`,`ACCOUNT_ID`,`SCAN_TYPE`, `GUARDDUTY_FINDING_IDSCAN_STATUS`,`RESOURCE_TYPE`,, `SCAN_START_TIME` e. Você pode alterar o *`max-results`* (até 50) e *`sort-criteria`* o. O `AttributeName` campo é obrigatório `sort-criteria` e deve ser definido como`scanStartTime`. No exemplo a seguir, os valores em *`red`* são espaços reservados. Substitua-os pelos valores apropriados para sua conta. Se você usar o `CriterionKey` mesmo que abaixo ListMalwareScans, certifique-se de substituir o exemplo `EqualsValue` pelo qual *`resource-type`* você deseja filtrar.

```
aws guardduty list-malware-scans --max-results 25 --sort-criteria
 '{"AttributeName": "scanStartTime", "OrderBy": "DESC"}' --filter-criteria
 '{"FilterCriterion":[{"CriterionKey":"RESOURCE_TYPE", "FilterCondition":
{"EqualsValue":"EBS_SNAPSHOT"}}] }'
```

```
aws guardduty get-malware-scan --scan-id abc123
```

- A resposta para o comando acima ListMalwareScans retornará até 25 escaneamentos com alguns detalhes sobre o (s) recurso (s) afetado (s). A resposta para o comando acima para GetMalwareScan retornará um único escaneamento com metadados detalhados sobre o escaneamento.

Monitorando escaneamentos usando EventBridge

EventBridge A Amazon é um serviço de ônibus de eventos sem servidor que facilita a conexão de seus aplicativos com dados de várias fontes. EventBridge fornece um fluxo de dados em tempo real de seus próprios aplicativos, aplicativos Software-as-a-Service (SaaS) e serviços da Amazon e encaminha esses dados para destinos como o Lambda. Isso permite monitorar eventos que ocorram em serviços e criem arquiteturas orientadas a eventos. Para obter mais informações, consulte o Guia EventBridge do usuário da Amazon.

GuardDuty publica EventBridge notificações no barramento de eventos padrão quando o status do escaneamento é determinado. Você pode configurar EventBridge regras em sua conta para enviar eventos para outros serviços integrados à Amazon EventBridge. O EventBridge preço padrão será aplicado. Para obter mais informações, consulte os EventBridge preços da Amazon.

Muitos dos valores mostrados abaixo são espaços reservados para o exemplo e variam de acordo com o escaneamento.

Eventos de resultados da verificação de malware

Valores potenciais do tipo de detalhe para Backup:

- “Resultado do EBS Snapshot Scan para proteção contra GuardDuty malware”
- “Resultado da verificação do EC2 AMI do GuardDuty Malware Protection”
- “Resultado da verificação do ponto de recuperação S3 do GuardDuty Malware Protection”
- “Resultado da verificação do EBS Recovery Point para proteção contra GuardDuty malware”
- “Resultado da verificação do ponto de recuperação do EC2 com proteção contra GuardDuty malware”

Exemplo de padrão de evento:

```
{
      "detail-type": ["GuardDuty Malware Protection EC2 AMI Scan Result"],
      "source": ["aws.guardduty"]
}
```

Exemplo de esquema de notificação para o EC2 AMI Scan sem ameaças encontradas:

```
{
    "version": "0",
    "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "detail-type": "GuardDuty Malware Protection EC2 AMI Scan Result",
    "source": "aws.guardduty",
    "account": "1111222233334444",
    "time": "2025-11-01T00:00:00Z",
    "region": "us-east-1",
    "resources": ["arn:aws:ec2:us-east-1:1111222233334444:image/
ami-1234567890abcdef0"],
    "detail": {
        "schemaVersion": "1.0",
        "scanStatus": "COMPLETED",
        "resourceType": "EC2_AMI",
        "scanId": "d41d8cd98f00b204e9800998ecf8427e",
        "scanStatusReason": null,
        "scanType": "ON_DEMAND",
        "triggerType": "GUARDDUTY",
        "scanCategory": "FULL_SCAN",
        "scanStartTime": 1234567890123,
        "scanCompleteTime": 2345678901234,
        "scanResultDetails": {
            "scanResultStatus": "NO_THREATS_FOUND",
            "uniqueThreatCount": null
        }
    }
}
```

Exemplo de esquema de notificação para o EC2 AMI Scan com ameaças encontradas:

```
{
    "version": "0",
    "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
    "detail-type": "GuardDuty Malware Protection EC2 AMI Scan Result",
    "source": "aws.guardduty",
```

```
    "account": "1111222233334444",
    "time": "2025-11-01T00:00:00Z",
    "region": "us-east-1",
    "resources": ["arn:aws:ec2:us-east-1:1111222233334444:image/
ami-1234567890abcdef0"],
    "detail": {
        "schemaVersion": "1.0",
        "scanStatus": "COMPLETED",
        "resourceType": "EC2_AMI",
        "scanId": "d41d8cd98f00b204e9800998ecf8427e",
        "scanStatusReason": null,
        "scanType": "ON_DEMAND",
        "triggerType": "GUARDDUTY",
        "scanCategory": "FULL_SCAN",
        "scanStartTime": 1234567890123,
        "scanCompleteTime": 2345678901234,
        "scanResultDetails": {
            "scanResultStatus": "THREATS_FOUND",
            "uniqueThreatCount": 1,
            "threats": {
                "name": "EICAR-Test-File (not a virus)",
                "source": "AMAZON",
                "count": 2,
                "itemDetails": [{
                    "resourceArn": "arn:aws:ec2:us-east-1:1111222233334444:snapshot/
snap-abcdef01234567890",
                    "hash":
 "e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855",
                    "itemPath": "/eicar.txt",
                    "additionalInfo": {
                        "versionId": null,
                        "deviceName": "/dev/sdf"
                    }
                }]
            }
        }
    }
}
```

Exemplo de esquema de notificação para verificação ignorada de AMI do EC2:

```
{
    "version": "0",
```

```
    "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE33333",
    "detail-type": "GuardDuty Malware Protection EC2 AMI Scan Result",
    "source": "aws.guardduty",
    "account": "111122223333444 4",
    "time": "2025-11-01T00:00:00Z",
    "region": "us-east-1",
    "resources": ["arn:aws:ec2:us-east-1:111122223333444 4:image/
ami-1234567890abcdef0"],
    "detail": {
        "schemaVersion": "1.0",
        "scanStatus": "SKIPPED",
        "resourceType": "EC2_AMI",
        "scanId": "d41d8cd98f00b204e9800998ecf8427e",
        "scanStatusReason": "UNSUPPORTED_AMI",
        "scanType": "ON_DEMAND",
        "triggerType": "GUARDDUTY",
        "scanCategory": "FULL_SCAN",
        "scanStartTime": 1234567890123,
        "scanCompleteTime": 2345678901234,
       "scanResultDetails": {
            "uniqueThreatCount": null,
            "threats": null
        }
    }
}
```

Cotas de proteção contra malware para backup

Proteção contra malware para cotas de backup

Nome da cota	AWS valor da cota padrão	É ajustável ?	Description
StartMalwareScan Limite de TPS para todos os tipos de recursos	10	Não	
Tamanho máximo de instantâneo suportado	2 TiB	Não	Esse limite se aplica ao tamanho total do instantâneo (`fullSnapshotSizeInBytes`), não ao tamanho incremental do instantân

Nome da cota	AWS valor da cota padrão	É ajustável ?	Description
			eo. Para obter mais informações, consulte Snapshot na Amazon EC2 API Reference. Para uma varredura incremental, GuardDuty ignora a verificação se o instantâneo atual ou o instantân eo base excederem esse limite.

Nome da cota	AWS valor da cota padrão	É ajustável ?	Description
Sistemas de arquivos compatíveis para varreduras de instantâneos e AMI	• Sistema de arquivos New Technology (NTFS) • Sistema de arquivos X (XFS) • Segundo sistema de arquivos estendido (ext2) • Quarto sistema de arquivos estendido (ext4) • Sistema de arquivos da tabela de alocação de arquivos (FAT) • Sistema de arquivos da tabela de alocação de arquivos virtuais (VFAT)	Não	

Nome da cota	AWS valor da cota padrão	É ajustável ?	Description
Número máximo de instantâneos em uma AMI com suporte para verificação de malware	40 para digitalização completa. Se houver mais de 40, GuardDuty digitalizará apenas 40 entre todos os instantâneos. Para uma varredura incremental, a varredura é ignorada.	Não	
Tamanho máximo de um objeto em um ponto de recuperação S3	100 GB	Não	O tamanho máximo do objeto S3 que GuardDuty tentará verificar se há malware.
Bytes de arquivo extraídos	100 GB	Não	A quantidade máxima de dados que GuardDuty podem ser extraídos e analisados de um arquivo. GuardDuty ignorará a extração de arquivos compactados para mais de 100 GB.

Nome da cota	AWS valor da cota padrão	É ajustável ?	Description
Arquivos extraídos	10.000	Não	O número máximo de arquivos que GuardDuty podem ser extraídos e analisados em um arquivo. Se o arquivo contiver mais de 10.000 arquivos, GuardDuty será necessário ignorar o arquivo arquivado. **Note** Os tipos de arquivos compostos estão potencial mente sujeitos a esses limites. Os tipos de arquivo incluem, mas não estão limitados a, mensagens de e-mail codificadas com Extensões MIME (Multipurpose Internet Mail Extensions), arquivos Python compilados (PYC), arquivos de ajuda em HTML compilado (CHM), todos os instaladores e documentos de formato (ODF). OpenDocument

Nome da cota	AWS valor da cota padrão	É ajustável ?	Description
Níveis máximos de profundidade de arquivo	5	Não	Os níveis máximos de arquivos aninhados que GuardDuty podem ser extraídos. Se o arquivamento incluir arquivos que estejam aninhados além desse valor, os arquivos aninhados GuardDuty serão ignorados.

GuardDuty Proteção RDS

> **Note**
>
> Você pode configurar a Proteção do RDS junto com todos os outros planos de proteção em uma única página no GuardDuty console. Para obter mais informações, consulte Configurando planos de proteção.

O RDS Protection na Amazon GuardDuty analisa e traça perfis de login e atividade de dados do RDS em busca de possíveis ameaças aos seus bancos de dados Amazon Aurora e RDS for PostgreSQL.

A Proteção do RDS para atividades de login analisa eventos de login em busca de possíveis ameaças de acesso aos bancos de dados Amazon Aurora (Amazon Aurora MySQL-Compatible Edition e Aurora Edition), RDS for PostgreSQL, Amazon RDS for MySQL e Amazon RDS for MariaDB. PostgreSQL-Compatible Ele ajuda você a identificar comportamentos de login potencialmente suspeitos nesses bancos de dados compatíveis. GuardDutymonitora e traça perfis contínuos em Atividade de login do RDS busca de atividades anômalas. Por exemplo, um agente externo não visto anteriormente tem acesso não autorizado ao seu banco de dados ou um adversário tenta obter acesso mediante uso de métodos de força bruta, adivinhando a senha do banco de dados.

O RDS Protection for data activity analisa padrões de consulta de banco de dados nos bancos de dados Amazon Aurora para PostgreSQL e RDS for PostgreSQL para detectar possíveis ameaças de acesso e manipulação de dados. GuardDuty monitora e traça perfis contínuos em Atividade de dados do RDS busca de comportamentos anômalos. Por exemplo, um ator lendo significativamente mais linhas do que o normal para esse banco de dados ou usuário, excluindo ou descartando dados ou acessando seu banco de dados a partir de um endereço IP conhecido como malicioso ou do Tor.

Para contas que ainda não habilitaram a Proteção RDS, você pode saber mais sobre 30-day free trial e optar por habilitar esse recurso. Para habilitar esse recurso, consulte Como habilitar a Proteção do RDS em ambientes com várias contas ou Como habilitar a Proteção do RDS para uma conta autônoma.

> **Observação**
>
> As instâncias de réplica de leitura do RDS para PostgreSQL exigem que a instância primária do banco de dados esteja em uma versão de banco de dados compatível e seja replicada

com êxito do banco de dados primário. Para obter mais informações sobre réplicas, consulte Como trabalhar com réplicas de leitura de banco de dados no Guia do usuário do Amazon RDS.

A Proteção do RDS não requer infraestrutura adicional. Ela foi projetada para não afetar o desempenho de suas instâncias de banco de dados. Quando o RDS Protection detecta uma tentativa de login potencialmente suspeita ou anômala, exfiltração ou atividade destrutiva de dados, GuardDuty gera uma ou mais com detalhes sobre o banco de dados potencialmente comprometido. Tipos de descoberta da Proteção do RDS

Avaliação gratuita de 30 dias

- Ao habilitar GuardDuty Conta da AWS em uma nova região pela primeira vez, você recebe um teste gratuito de 30 dias. Nesse caso, GuardDuty também ativa o RDS Protection, que está incluído no teste gratuito. O monitoramento da atividade de login do RDS Protection e o monitoramento da atividade de dados do RDS Protection começarão a monitorar a atividade de seus bancos de dados.
- Quando você já estiver usando GuardDuty e decidir ativar a Proteção do RDS em uma nova região pela primeira vez, sua conta nessa região receberá um teste gratuito de 30 dias da Proteção do RDS.
- Quando você já estiver usando o RDS Protection para atividades de login em um Conta da AWS e decidir ativar o RDS Protection para atividades de dados pela primeira vez, sua conta receberá um teste gratuito de 30 dias do RDS Protection para atividades de dados.
- Você pode optar por desativar a Proteção RDS ou o monitoramento da atividade de dados da Proteção RDS em qualquer região a qualquer momento.
- Durante a avaliação gratuita de 30 dias, é possível obter uma estimativa de seus custos de uso para essa conta e região. Após o término da avaliação gratuita de 30 dias, a Proteção do RDS não será desabilitada automaticamente. Nessa região, haverá custos de uso a serem incorridos em sua conta. Para obter mais informações, consulte Monitorando GuardDuty o uso e estimando custos.

Quando o recurso de Proteção RDS não está ativado, GuardDuty não detecta comportamento anômalo ou suspeito de login ou dados. Se você desabilitar a Proteção do RDS, interromperá GuardDuty imediatamente o monitoramento da atividade do RDS e não detectará nenhuma ameaça potencial às suas instâncias de banco de dados suportadas nem gerará os tipos de descoberta associados.

Para saber Regiões da AWS onde os bancos de dados Aurora PostgreSQL Limitless são compatíveis, consulte Requisitos para o banco de dados Aurora PostgreSQL Limitless.

Bancos de dados do Amazon Aurora, Amazon RDS e Aurora Limitless Databases compatíveis

A tabela a seguir mostra as versões compatíveis do banco de dados Aurora e Amazon RDS para monitoramento de atividades de login e monitoramento de atividades de dados do RDS Protection. GuardDuty pode se expandir para bancos de dados adicionais do Amazon RDS no futuro.

Mecanismo do banco de dados do Amazon RDS e Amazon Aurora	Versões de mecanismo compatíveis com monitoramento de atividades de login	Versões de mecanismo compatíveis com monitoramento de atividades de dados
Aurora MySQL	• 2.10.2 ou posterior • 3.02.1 ou posterior • Versões principais subsequentes	Não compatível
Aurora PostgreSQL	• 10.23 ou posterior • 11.12 ou posterior • 12.7 ou posterior • 13.3 ou posterior • 14.3 ou posterior • 15.2 ou posterior • 16.1 ou posterior • Versões principais subsequentes	• 11.19 ou posterior • 12.14 ou posterior • 13.10 ou posterior • 14.7 ou posterior • 15.2 ou posterior • Versões principais subsequentes
RDS para PostgreSQL	• 11.17 ou posterior • 12.12 ou posterior • 13.8 ou posterior • 14.5 ou posterior	• 11.20 ou posterior • 12.15 ou posterior • 13.11 ou posterior • 14.8 ou posterior • 15.3 ou posterior

Mecanismo do banco de dados do Amazon RDS e Amazon Aurora	Versões de mecanismo compatíveis com monitoramento de atividades de login	Versões de mecanismo compatíveis com monitoramento de atividades de dados
	• RDS para PostgreSQL versão 15 • RDS para PostgreSQL versão 16 • RDS para PostgreSQL versão 17 • RDS para PostgreSQL versão 18 • Versões principais subsequentes	• Versões principais subsequentes
Banco de dados sem limite Amazon Aurora PostgreSQL	• `16.4-limitless` • Versões principais subsequentes	Não compatível
Amazon RDS para MariaDB	• 10.6.25 ou posterior • 10.11.16 ou posterior • 11.4.10 ou posterior • 11.8.6 ou posterior • Versões principais subsequentes	Não compatível
Amazon RDS para MySQL	• 8.0.45 ou posterior • 8.4.8 ou posterior • Versões principais subsequentes	Não compatível

Atividade de login do RDS

Quando você ativa o recurso RDS Protection, inicia GuardDuty automaticamente o monitoramento da atividade de login do RDS para seus bancos de dados, diretamente dos serviços Aurora e Amazon

RDS. A atividade de login do RDS captura as tentativas de login bem-sucedidas e malsucedidas feitas Bancos de dados do Amazon Aurora, Amazon RDS e Aurora Limitless Databases compatíveis no seu AWS ambiente. Se houver uma indicação de comportamento anômalo de login, GuardDuty gera uma descoberta com detalhes sobre o banco de dados potencialmente comprometido. Ao habilitar a Proteção do RDS pela primeira vez ou ao ter uma instância de banco de dados recém-criada, há um período de aprendizado para estabelecer a linha de base do comportamento normal. Por essa razão, instâncias de banco de dados recém-habilitadas ou recém-criadas podem não ter uma descoberta de login anômala associada por até duas semanas.

Quando o RDS Protection detecta uma ameaça potencial, como um padrão incomum em uma série de tentativas de login bem-sucedidas, malsucedidas ou incompletas, GuardDuty gera uma ou mais. Tipos de descoberta da Proteção do RDS Com base no tipo de descoberta, pode incluir detalhes sobre o comportamento anômalo, como. Anomalias baseadas na atividade de login do RDS GuardDuty não disponibiliza registros de atividades de login do RDS para você.

Atividade de dados do RDS

Quando você ativa a Proteção do RDS para atividades de dados, GuardDuty analisa os padrões de atividade do banco de dados nos bancos de dados compatíveis do Aurora e do Amazon RDS para identificar possíveis ameaças de acesso e manipulação de dados. Se ele detectar uma atividade anômala de dados, GuardDuty gera uma descoberta com detalhes sobre o banco de dados potencialmente comprometido. Quando você ativa a Proteção do RDS para atividades de dados pela primeira vez ou quando cria uma nova instância de banco de dados, há um período de aprendizado de até duas semanas para estabelecer uma linha de base do comportamento normal. Durante esse período, talvez você não tenha uma descoberta anômala de atividade de dados associada.

Quando a Proteção RDS para atividades de dados detecta uma ameaça potencial, GuardDuty gera uma ou mais. Tipos de descoberta da Proteção do RDS Os exemplos incluem um ator lendo significativamente mais linhas do que o normal para esse banco de dados ou usuário, excluindo ou descartando dados ou acessando seu banco de dados a partir de um endereço IP conhecido como malicioso ou do Tor. Dependendo do tipo de descoberta, a descoberta pode incluir detalhes sobre o comportamento anômalo, como. Anomalias baseadas em atividades de dados do RDS GuardDuty não disponibiliza registros de atividades de dados do RDS para você.

Como habilitar a Proteção do RDS em ambientes com várias contas

Em um ambiente de várias contas, somente a conta de GuardDuty administrador delegado tem a opção de ativar ou desativar o recurso de Proteção do RDS, incluindo a configuração adicional de monitoramento da atividade de dados do RDS, para as contas membros em sua organização. As contas GuardDuty dos membros não podem modificar essa configuração em suas contas. A conta de GuardDuty administrador delegado gerencia suas contas de membros usando AWS Organizations. Essa conta de GuardDuty administrador delegado pode optar por habilitar automaticamente o monitoramento da atividade de login do RDS e o monitoramento da atividade de dados do RDS para todas as novas contas à medida que elas ingressam na organização. Para obter mais informações sobre ambientes com várias contas, consulte Gerenciar várias contas.

Ativando a Proteção RDS para uma conta de administrador delegado GuardDuty

Escolha seu método de acesso preferido para ativar a Proteção do RDS, incluindo a configuração adicional de monitoramento da atividade de dados do RDS, para a conta do administrador delegado GuardDuty .

Console

1. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.
2. No painel de navegação, escolha Planos de proteção.
3. Escolha Configurar todas as habilitações.
4. Em Proteção do RDS, localize as entradas RDS Login Activity Monitoring e RDS Data Activity Monitoring.
5. Na coluna Esta conta, escolha Ativada para cada entrada que você deseja ativar ou Não habilitada para deixá-la desativada.

> **Note**
>
> O RDS Login Activity Monitoring deve estar ativado antes que você possa habilitar o RDS Data Activity Monitoring.

API/CLI

Execute a operação da API updateDetector usando seu próprio ID de detector regional e transmitindo o `name` do objeto `features` como `RDS_LOGIN_EVENTS` e `status` como `ENABLED`. Para também ativar o monitoramento da atividade de dados do RDS, passe `name` abaixo `AdditionalConfiguration` com `status` definido `RDS_DATA_RISK` como. `ENABLED`

Como alternativa, você pode usar AWS CLI para ativar a Proteção RDS. Execute o comando a seguir e *`12abc34d567e8fa901bc2d34e56789f0`* substitua pelo ID do detector da sua conta e *`us-east-1`* pela região em que você deseja ativar a Proteção RDS.

Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no https://console.aws.amazon.com/guardduty/console ou execute a ListDetectorsAPI.

O exemplo a seguir ativa o monitoramento da atividade de login do RDS na conta do administrador delegado e usa `AdditionalConfiguration` para habilitar também o monitoramento da atividade de dados do RDS:

```
aws guardduty update-detector \
    --detector-id 12abc34d567e8fa901bc2d34e56789f0 \
    --region us-east-1 \
    --features '[
        {
            "Name": "RDS_LOGIN_EVENTS",
            "Status": "ENABLED",
            "AdditionalConfiguration": [
                {
                    "Name": "RDS_DATA_RISK",
                    "Status": "ENABLED"
                }
            ]
        }
    ]'
```

Auto-enable Proteção RDS para todas as contas de membros

Escolha seu método de acesso preferido para ativar o recurso de Proteção do RDS, incluindo a configuração adicional de monitoramento da atividade de dados do RDS, para todas as contas dos membros. Isso inclui contas-membro existentes e as novas contas que ingressam na organização.

Console

1. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.

   Certifique-se de usar as credenciais da conta de GuardDuty administrador delegado.
2. No painel de navegação, escolha Planos de proteção.
3. Escolha Configurar todas as habilitações.
4. Em Proteção do RDS, escolha Habilitar para todas as contas. Essa ação habilita automaticamente a Proteção do RDS para contas novas e existentes na organização.
5. Para também ativar o monitoramento de atividades de dados do RDS para cada conta, expanda Configuração adicional e escolha Habilitar para todas as contas para o RDS Data Activity Monitoring.
6. Escolha Salvar tudo e, em seguida, escolha Confirmar e salvar.

> **Note**
>
> Pode levar até 24 horas para atualizar a configuração das contas-membro.

API/CLI

Para habilitar a Proteção RDS para todas as contas membros em sua organização, incluindo membros existentes e novas contas que ingressarão posteriormente, invoque a operação da UpdateOrganizationConfigurationAPI usando a sua própria. *`detector ID`* `AutoEnable`Defina como `ALL` para o `RDS_LOGIN_EVENTS` recurso e passe `RDS_DATA_RISK` abaixo `AdditionalConfiguration` com `AutoEnable` set to `ALL` para também ativar automaticamente o monitoramento da atividade de dados do RDS.

Como alternativa, você pode usar AWS CLI para ativar a Proteção RDS. Execute o comando a seguir e *`12abc34d567e8fa901bc2d34e56789f0`* substitua pelo ID do detector da sua conta e *`us-east-1`* pela região em que você deseja ativar a Proteção RDS.

Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no https://console.aws.amazon.com/guardduty/console ou execute a ListDetectorsAPI.

O exemplo a seguir ativa automaticamente ambas `RDS_LOGIN_EVENTS` e `RDS_DATA_RISK` para cada conta de membro na organização:

```
aws guardduty update-organization-configuration \
    --detector-id 12abc34d567e8fa901bc2d34e56789f0 \
    --region us-east-1 \
    --auto-enable-organization-members ALL \
    --features '[
        {
            "Name": "RDS_LOGIN_EVENTS",
            "AutoEnable": "ALL",
            "AdditionalConfiguration": [
                {
                    "Name": "RDS_DATA_RISK",
                    "AutoEnable": "ALL"
                }
            ]
        }
    ]'
```

> **Note**
>
> Pode levar até 24 horas para atualizar a configuração das contas-membro.

Habilitar a Proteção do RDS para todas as contas-membro ativas existentes

Escolha seu método de acesso preferido para ativar a Proteção RDS, incluindo a configuração adicional de monitoramento de atividades de dados do RDS, para todas as contas de membros ativas existentes em sua organização. As contas de membros que já foram GuardDuty ativadas são chamadas de membros ativos existentes.

> **Note**
>
> O RDS Login Activity Monitoring deve estar ativado em uma conta de membro antes que você possa habilitar o RDS Data Activity Monitoring nessa conta.

Console

1. Faça login no Console de gerenciamento da AWS e abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.

Faça login usando as credenciais da conta de GuardDuty administrador delegado.

2. No painel de navegação, selecione Contas.
3. Na página Contas, selecione as contas de membros ativos existentes que você deseja ativar. Para selecionar cada conta, use a caixa de seleção no cabeçalho da tabela.
4. No menu suspenso Editar planos de proteção, escolha Atividade de login do RDS e, em seguida, escolha Habilitar.
5. Para também ativar o monitoramento da atividade de dados do RDS nas contas selecionadas, abra o menu suspenso Editar planos de proteção novamente, escolha Atividade de dados do RDS e escolha Habilitar. O monitoramento de atividades de login do RDS já deve estar ativado em cada conta selecionada.

API/CLI

Execute a operação updateMemberDetectorsda API usando a sua própria*detector ID*. Passe `RDS_DATA_RISK` de `AdditionalConfiguration` lado o `RDS_LOGIN_EVENTS` recurso para controlar também o monitoramento da atividade de dados do RDS.

Como alternativa, você pode usar AWS CLI para ativar a Proteção RDS. Execute o comando a seguir e *12abc34d567e8fa901bc2d34e56789f0* substitua pelo ID do detector da sua conta e *us-east-1* pela região em que você deseja ativar a Proteção RDS.

Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no https://console.aws.amazon.com/guardduty/console ou execute a ListDetectorsAPI.

O exemplo a seguir permite o monitoramento da atividade de login do RDS em uma conta de membro ativa existente e também `AdditionalConfiguration` permite o monitoramento da atividade de dados do RDS:

```
aws guardduty update-member-detectors \
    --detector-id 12abc34d567e8fa901bc2d34e56789f0 \
    --region us-east-1 \
    --account-ids 111122223333 \
    --features '[
        {
            "Name": "RDS_LOGIN_EVENTS",
            "Status": "ENABLED",
```

```
            "AdditionalConfiguration": [
                {
                    "Name": "RDS_DATA_RISK",
                    "Status": "ENABLED"
                }
            ]
        }
    ]'
```

Também é possível passar uma lista de IDs de conta separados por um espaço.

Quando o código é executado com êxito, ele retorna uma lista vazia de `UnprocessedAccounts`. Se houver algum problema na alteração das configurações do detector de uma conta, esse ID de conta será listado junto com um resumo do problema.

Auto-enable Proteção RDS para contas de novos membros

Escolha seu método de acesso preferido para habilitar o monitoramento da atividade de login do RDS e o monitoramento da atividade de dados do RDS para novas contas que ingressam na sua organização.

Console

1. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.

   Certifique-se de usar as credenciais da conta de GuardDuty administrador delegado.
2. No painel de navegação, escolha Planos de proteção.
3. Escolha Configurar todas as habilitações.
4. Escolha Configurar contas manualmente.
5. Em Proteção do RDS, selecione Ativar automaticamente para novas contas de membros. Essa etapa garante que, sempre que uma nova conta ingressar na sua organização, a Proteção do RDS seja habilitada automaticamente para a conta dessa pessoa. Somente a conta do GuardDuty administrador delegado da organização pode modificar essa configuração.
6. Para também ativar automaticamente o monitoramento de atividades de dados do RDS para novas contas, expanda Configuração adicional e selecione Ativar automaticamente para novas contas de membros para o RDS Data Activity Monitoring.
7. Escolha Salvar.

API/CLI

Para ativar automaticamente a Proteção do RDS para novas contas que ingressam na sua organização, invoque a operação da UpdateOrganizationConfigurationAPI usando a sua própria. *detector ID* `AutoEnable`Defina como `NEW` para o `RDS_LOGIN_EVENTS` recurso e passe `RDS_DATA_RISK` abaixo `AdditionalConfiguration` com `AutoEnable` set to `NEW` para também ativar automaticamente o monitoramento da atividade de dados do RDS. Para parar de ativar automaticamente um recurso para novas contas, defina `NONE` seu `AutoEnable` valor como.

Como alternativa, você pode usar AWS CLI para ativar a Proteção RDS. Execute o comando a seguir e *12abc34d567e8fa901bc2d34e56789f0* substitua pelo ID do detector da sua conta e *us-east-1* pela região em que você deseja ativar a Proteção RDS.

Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no https://console.aws.amazon.com/guardduty/console ou execute a ListDetectorsAPI.

O exemplo a seguir ativa automaticamente ambas `RDS_LOGIN_EVENTS` e `RDS_DATA_RISK` para novas contas que ingressam na organização:

```
aws guardduty update-organization-configuration \
    --detector-id 12abc34d567e8fa901bc2d34e56789f0 \
    --region us-east-1 \
    --auto-enable-organization-members NEW \
    --features '[
        {
            "Name": "RDS_LOGIN_EVENTS",
            "AutoEnable": "NEW",
            "AdditionalConfiguration": [
                {
                    "Name": "RDS_DATA_RISK",
                    "AutoEnable": "NEW"
                }
            ]
        }
    ]'
```

Habilitar ou desabilitar seletivamente a Proteção do RDS para contas de membros

Escolha seu método de acesso preferido para habilitar seletivamente o monitoramento da atividade de login do RDS e da atividade de dados do RDS para contas de membros.

Console

1. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.

   Certifique-se de usar as credenciais da conta de GuardDuty administrador delegado.
2. No painel de navegação, selecione Contas.

   Na página Contas, revise as colunas Atividade de login do RDS e Atividade de dados do RDS para ver o status da sua conta de membro.
3. Para habilitar ou desabilitar seletivamente a atividade de login do RDS

   Selecione a conta para a qual deseja configurar a Proteção do RDS. Você pode selecionar várias contas ao mesmo tempo. No menu suspenso Editar planos de proteção, escolha Atividade de login do RDS e escolha a opção apropriada.
4. Para ativar ou desativar seletivamente a atividade de dados do RDS

   Selecione a conta para a qual você deseja configurar o monitoramento da atividade de dados do RDS. Você pode selecionar várias contas ao mesmo tempo. No menu suspenso Editar planos de proteção, escolha Atividade de dados do RDS e escolha a opção apropriada.

API/CLI

Para ativar ou desativar seletivamente a Proteção RDS para suas contas de membros, invoque a operação da updateMemberDetectorsAPI usando a sua própria. *`detector ID`* `RDS_DATA_RISK`Transmita `AdditionalConfiguration` o `RDS_LOGIN_EVENTS` recurso para controlar o monitoramento da atividade de dados do RDS de forma independente.

Como alternativa, você pode usar AWS CLI para ativar a Proteção RDS. Execute o comando a seguir e *`12abc34d567e8fa901bc2d34e56789f0`* substitua pelo ID do detector da sua conta e *`us-east-1`* pela região em que você deseja ativar a Proteção RDS.

Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no https://console.aws.amazon.com/guardduty/console ou execute a ListDetectorsAPI.

O exemplo a seguir habilita RDS_LOGIN_EVENTS e RDS_DATA_RISK:

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --region us-east-1 --account-ids 111122223333 --features '[{"Name":
 "RDS_LOGIN_EVENTS", "Status": "ENABLED", "AdditionalConfiguration": [{"Name":
 "RDS_DATA_RISK", "Status": "ENABLED"}]}]'
```

Para manter o monitoramento da atividade de login do RDS ativado enquanto desativa o monitoramento da atividade de dados do RDS, RDS_LOGIN_EVENTS `Status` defina como ENABLED e RDS_DATA_RISK `Status` para: DISABLED

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --region us-east-1 --account-ids 111122223333 --features '[{"Name":
 "RDS_LOGIN_EVENTS", "Status": "ENABLED", "AdditionalConfiguration": [{"Name":
 "RDS_DATA_RISK", "Status": "DISABLED"}]}]'
```

> **Note**
>
> Também é possível passar uma lista de IDs de conta separados por um espaço.

Quando o código é executado com êxito, ele retorna uma lista vazia de `UnprocessedAccounts`. Se houver algum problema na alteração das configurações do detector de uma conta, esse ID de conta será listado junto com um resumo do problema.

Como habilitar a Proteção do RDS para uma conta autônoma

Uma conta autônoma é responsável pela decisão de ativar ou desativar um plano de proteção Conta da AWS em uma conta específica Região da AWS.

Se sua conta estiver associada a uma conta de GuardDuty administrador por meio AWS Organizations ou pelo método de convite, esta seção não se aplica à sua conta. Para obter mais informações, consulte Como habilitar a Proteção do RDS em ambientes com várias contas.

Depois de ativar a Proteção RDS, GuardDuty iniciará o monitoramento dos bancos Atividade de login do RDS de dados compatíveis em sua conta.

Selecione o método de acesso de sua preferência para configurar a Proteção do RDS para uma conta autônoma.

Console

1. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.
2. No painel de navegação, escolha Planos de proteção.
3. Escolha Configurar todas as habilitações. Em Proteção do RDS, escolha Habilitar para ativar a Proteção do RDS.
4. Escolha Salvar tudo e, em seguida, escolha Confirmar e salvar.

API/CLI

Execute a operação da API updateDetector usando seu próprio ID de detector regional e transmitindo o `name` do objeto `features` como `RDS_LOGIN_EVENTS` e `status` como `ENABLED`. Para também ativar o monitoramento da atividade de dados do RDS, passe `name` abaixo `AdditionalConfiguration` com `status` definido `RDS_DATA_RISK` como. `ENABLED`

Como alternativa, você pode usar AWS CLI para ativar a Proteção RDS. Execute o comando a seguir e *`12abc34d567e8fa901bc2d34e56789f0`* substitua pelo ID do detector da sua conta e *`us-east-1`* pela região em que você deseja ativar a Proteção RDS.

Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no https://console.aws.amazon.com/guardduty/console ou execute a ListDetectorsAPI.

O exemplo a seguir habilita `RDS_LOGIN_EVENTS` e `RDS_DATA_RISK`:

```
aws guardduty update-detector \
    --detector-id 12abc34d567e8fa901bc2d34e56789f0 \
    --region us-east-1 \
    --features '[
        {
            "Name": "RDS_LOGIN_EVENTS",
            "Status": "ENABLED",
            "AdditionalConfiguration": [
                {
                    "Name": "RDS_DATA_RISK",
                    "Status": "ENABLED"
                }
            ]
        }
```

```
    ]'
```

Solução de problemas de monitoramento da Proteção do RDS

GuardDuty O RDS Protection analisa e traça o perfil de sua atividade de login do RDS em busca de possíveis ameaças de acesso ao. Bancos de dados compatíveis Para coletar a telemetria de segurança de forma eficaz, é GuardDuty necessário que seu banco de dados esteja configurado e opere sem problemas. Se seu banco de dados estiver configurado incorretamente ou apresentar problemas, o monitoramento de segurança poderá ser afetado.

A seção a seguir fornece problemas comuns e etapas para solucioná-los.

Armazenamento do RDS cheio

Quando sua instância do RDS ficar sem armazenamento, GuardDuty talvez não colete a telemetria de segurança. Atingir a alocação de capacidade de armazenamento de instância de banco de dados (`storage-full`) é um status crítico e o RDS recomenda corrigir esse problema imediatamente. Para obter mais informações, consulte Visualizar status de instância no Guia do usuário do Amazon RDS.

Para resolver o status `storage-full`, é possível executar uma das seguintes ações:

- Habilitar o escalonamento automático de armazenamento (recomendado) – habilite o escalonamento automático de armazenamento do Amazon RDS para gerenciar automaticamente a capacidade de armazenamento e evitar condições futuras de `storage-full`. Para mais informações, consulte Gerenciar a capacidade automaticamente com o dimensionamento automático de armazenamento do Amazon RDS no Guia do usuário do Amazon RDS.
- Monitorar a utilização do armazenamento – verifique a utilização do armazenamento usando um dos seguintes métodos:
  - Use CloudWatch métricas para ver detalhes sobre o armazenamento. Para obter mais informações, consulte CloudWatch Database Insights no Guia CloudWatch do usuário da Amazon.
  - Veja as métricas de armazenamento seguindo as etapas em Monitorar métricas em uma instância do Amazon RDS no Guia do usuário do Amazon RDS.
- Modifique a capacidade de armazenamento – para obter informações sobre como aumentar a capacidade de armazenamento da sua instância, consulte Aumentar a capacidade de armazenamento da instância de banco de dados no Guia do usuário do Amazon RDS.

Versões não compatíveis no banco de dados primário do RDS for PostgreSQL

As instâncias de réplica de leitura do RDS para PostgreSQL exigem que a instância primária do banco de dados esteja na versão compatível e seja replicada com êxito do banco de dados primário. GuardDuty monitora suas instâncias somente quando esses requisitos são atendidos.

Para resolver o problema de versão incompatível, execute um dos seguintes procedimentos:

- Verifique a compatibilidade da versão do banco de dados – verifique se seu banco de dados principal do RDS para PostgreSQL está executando uma das versões compatíveis. Para obter mais informações, consulte Bancos de dados compatíveis.
- Solucione possíveis problemas de replicação – revise e resolva quaisquer problemas de replicação entre as instâncias primária e de réplica. Para mais informações sobre como fazer isso, consulte Trabalhar com réplicas de leitura do RDS para PostgreSQL no Guia do usuário do Amazon RDS.

Considerações adicionais sobre segurança

Se sua organização tiver requisitos rígidos de conformidade, recomendamos implementar a auditoria de banco de dados, além de usar a Proteção do RDS. Para obter mais informações sobre suas responsabilidades de segurança e modelo de responsabilidade compartilhada, consulte Segurança no Amazon RDS no Guia do usuário do Amazon RDS.

GuardDuty Proteção Lambda

> **Note**
>
> Você pode configurar o Lambda Protection junto com todos os outros planos de proteção em uma única página no GuardDuty console. Para obter mais informações, consulte Configurando planos de proteção.

A Proteção do Lambda ajuda você a identificar possíveis ameaças à segurança quando uma função do AWS Lambda é invocada em seu ambiente da AWS . Quando você ativa a Proteção Lambda, GuardDuty começa a monitorar os registros de atividades da rede Lambda. Isso inclui Logs de fluxo da VPC de todas as funções do Lambda da sua conta (incluindo os logs que não usam redes VPC) e os logs que são gerados quando a função do Lambda é invocada. Quando GuardDuty identifica tráfego de rede suspeito que é indicativo da presença de um código potencialmente malicioso em sua função Lambda, GuardDuty gera um ou mais. Tipos de descoberta da Proteção do Lambda

Avaliação gratuita de 30 dias

A lista a seguir explica como a avaliação gratuita de 30 dias funciona para a sua conta:

- Ao habilitar GuardDuty Conta da AWS em uma nova região pela primeira vez, você recebe um teste gratuito de 30 dias. Nesse caso, também GuardDuty habilitará o Lambda Protection, que está incluído no teste gratuito.
- Quando você já estiver usando GuardDuty e decidir ativar o Lambda Protection pela primeira vez, sua conta nessa região receberá um teste gratuito de 30 dias do Lambda Protection.
- É possível optar por desabilitar a Proteção Lambda em qualquer região a qualquer momento.
- Durante a avaliação gratuita de 30 dias, é possível obter uma estimativa de seus custos de uso nessa conta e região. Após o término da avaliação gratuita de 30 dias, a Proteção Lambda não é desabilitada automaticamente. Sua conta nessa região começará a incorrer em custos de uso. Para obter mais informações, consulte Monitorando GuardDuty o uso e estimando custos.

Os logs de atividade de rede Lambda estão sujeitos a alterações, incluindo a expansão para outras atividades de rede, como dados de consulta ao DNS gerados pela invocação das funções do Lambda. A expansão para outras formas de monitoramento de atividades de rede aumentará o volume de dados que GuardDuty serão processados para a Proteção Lambda. Isso afetará

diretamente o custo de uso da Proteção do Lambda. Sempre que GuardDuty começar a monitorar um registro adicional de atividades de rede, ele fornecerá um aviso às contas que ativaram a Proteção Lambda, pelo menos 30 dias antes do lançamento.

> **Note**
>
> O Monitoramento de atividades de rede do Lambda não inclui os registros das funções do Lambda@Edge.

Monitoramento de atividades da rede Lambda

Quando você ativa a Proteção Lambda, monitora os registros de atividades GuardDuty da rede Lambda que são gerados quando uma função do Lambda, associada à sua conta, é invocada. Isso ajuda você a detectar possíveis ameaças à segurança da função do Lambda. Para funções Lambda configuradas para usar redes VPC, você não precisa habilitar registros de fluxo de VPC para as interfaces de rede elástica (ENI) criadas pelo Lambda for. GuardDuty GuardDuty cobra apenas pela quantidade de dados de registros de atividades da rede Lambda processados (em GB) para gerar uma descoberta. GuardDuty otimiza os custos aplicando filtros inteligentes e analisando um subconjunto dos registros de atividades da rede Lambda que são relevantes para a detecção de ameaças.

GuardDuty não gerencia seus registros de atividades da rede Lambda (incluindo registros de fluxo VPC e não VPC) nem os torna acessíveis em sua conta.

Como habilitar a proteção Lambda em ambientes com várias contas

Em um ambiente com várias contas, somente a conta do GuardDuty administrador delegado tem a opção de ativar ou desativar a Proteção Lambda para as contas dos membros em sua organização. As contas GuardDuty dos membros não podem modificar essa configuração em suas contas. A conta de GuardDuty administrador delegado gerencia as contas dos membros usando AWS Organizations. A conta de GuardDuty administrador delegado pode optar por habilitar automaticamente o Lambda Network Activity Monitoring para todas as novas contas à medida que elas ingressam na organização. Para obter mais informações sobre ambientes com várias contas, consulte Gerenciamento de várias contas na Amazon. GuardDuty

Habilitando a Proteção Lambda para uma conta de administrador delegado GuardDuty

Escolha seu método de acesso preferido para ativar ou desativar o Lambda Network Activity Monitoring para uma conta de administrador delegado GuardDuty .

Console

1. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.
2. No painel de navegação, em Configurações, escolha Proteção do Lambda.
3. Na página Proteção do Lambda, escolha Editar.
4. Execute um destes procedimentos:

   Como usar a opção Habilitar para todas as contas

   - Escolha Habilitar para todas as contas. Isso habilitará o plano de proteção para todas as GuardDuty contas ativas em sua AWS organização, incluindo as novas contas que ingressam na organização.
   - Escolha Salvar.

   Como usar a opção Configurar contas manualmente

   - Para ativar o plano de proteção somente para a conta de GuardDuty administrador delegado, escolha Configurar contas manualmente.
   - Escolha Habilitar na seção Conta de GuardDuty administrador delegado (esta conta).
   - Escolha Salvar.

API/CLI

Execute a operação da API updateDetector usando seu próprio ID de detector regional e transmitindo o `name` do objeto `features` como `LAMBDA_NETWORK_LOGS` e `status` como`ENABLED`.

Como alternativa, você pode usar AWS CLI para ativar a Proteção Lambda. Execute o comando a seguir e *`12abc34d567e8fa901bc2d34e56789f0`* substitua pelo ID do detector da sua conta e *`us-east-1`* pela região em que você deseja ativar a Proteção Lambda.

Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no https://console.aws.amazon.com/guardduty/console ou execute a ListDetectorsAPI.

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
region us-east-1 --features '[{"Name": "LAMBDA_NETWORK_LOGS", "Status": "ENABLED"}]'
```

Auto-enable Monitoramento de atividades da rede Lambda para todas as contas dos membros

Escolha seu método de acesso preferido para habilitar o recurso Monitoramento de atividades de rede do Lambda para todas as contas-membro. Isso inclui contas-membro existentes e as novas contas que ingressam na organização.

Console

1. Faça login no Console de gerenciamento da AWS e abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.

   Certifique-se de usar as credenciais da conta de GuardDuty administrador delegado.

2. Execute um destes procedimentos:

   Usando a página Planos de Proteção

   1. No painel de navegação, escolha Planos de proteção.
   2. Escolha Configurar todas as habilitações.
   3. Em Proteção Lambda, escolha Ativar para todas as contas. Essa ação habilita automaticamente o Monitoramento de atividades de rede do Lambda para contas existentes e novas na organização.
   4. Escolha Salvar tudo e, em seguida, escolha Confirmar e salvar.

   > **Note**
   >
   > Pode levar até 24 horas para atualizar a configuração das contas-membro.

Como usar a página Contas

1. No painel de navegação, selecione Contas.
2. Na página Contas, escolha Auto-enableas preferências antes de Adicionar contas por convite.
3. Na janela Gerenciar preferências de habilitação automática, escolha Habilitar para todas as contas em Monitoramento de atividades de rede do Lambda.

   > **Note**
   >
   > Por padrão, essa ação ativa automaticamente a opção Auto-enable GuardDuty para novas contas de membros.

4. Escolha Salvar.

Se você não conseguir usar a opção Habilitar para todas as contas, consulte Habilite ou desabilite seletivamente o Monitoramento de atividades de rede do Lambda para contas-membro.

API/CLI

Para ativar ou desativar seletivamente o Lambda Network Activity Monitoring para suas contas de membros, invoque a operação updateMemberDetectorsda API usando a sua própria. *detector ID*

Como alternativa, você pode usar AWS CLI para ativar a Proteção Lambda. Execute o comando a seguir e *12abc34d567e8fa901bc2d34e56789f0* substitua pelo ID do detector da sua conta e *us-east-1* pela região em que você deseja ativar a Proteção Lambda.

Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no https://console.aws.amazon.com/guardduty/console ou execute a ListDetectorsAPI.

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --account-ids 111122223333 --region us-east-1--features '[{"Name":
 "LAMBDA_NETWORK_LOGS", "Status": "ENABLED"}]'
```

Também é possível passar uma lista de IDs de conta separados por um espaço.

Quando o código é executado com êxito, ele retorna uma lista vazia de `UnprocessedAccounts`. Se houver algum problema na alteração das configurações do detector de uma conta, esse ID de conta será listado junto com um resumo do problema.

Habilite o monitoramento de atividades da rede Lambda para todas as contas-membro ativas existentes

Escolha seu método de acesso preferido para habilitar o Monitoramento de atividades de rede do Lambda para todas as contas-membro ativas existentes na organização.

Console

Para configurar o Monitoramento de atividades de rede do Lambda para todas as contas-membro ativas existentes

1. Faça login no Console de gerenciamento da AWS e abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.

   Faça login usando as credenciais da conta de GuardDuty administrador delegado.
2. No painel de navegação, escolha Planos de proteção.
3. Escolha Configurar todas as habilitações. Em Proteção Lambda, você pode ver o status atual da configuração. Na seção Contas-membro ativas, escolha Ações.
4. No menu suspenso Ações, escolha Habilitar para todas as contas-membro ativas existentes.
5. Escolha Confirmar.

API/CLI

Para ativar ou desativar seletivamente o Lambda Network Activity Monitoring para suas contas de membros, invoque a operação updateMemberDetectorsda API usando a sua própria. *`detector ID`*

Como alternativa, você pode usar AWS CLI para ativar a Proteção Lambda. Execute o comando a seguir e *`12abc34d567e8fa901bc2d34e56789f0`* substitua pelo ID do detector da sua conta e *`us-east-1`* pela região em que você deseja ativar a Proteção Lambda.

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --region us-east-1 --account-ids 111122223333 --features '[{"Name":
 "LAMBDA_NETWORK_LOGS", "Status": "ENABLED"}]'
```

Também é possível passar uma lista de IDs de conta separados por um espaço.

Quando o código é executado com êxito, ele retorna uma lista vazia de `UnprocessedAccounts`. Se houver algum problema na alteração das configurações do detector de uma conta, esse ID de conta será listado junto com um resumo do problema.

Auto-enable Monitoramento de atividades da rede Lambda para novas contas de membros

Escolha seu método de acesso preferido para habilitar o Monitoramento de atividades de rede do Lambda para novas contas que ingressam na sua organização.

Console

A conta de GuardDuty administrador delegado pode habilitar o Lambda Network Activity Monitoring para novas contas de membros em uma organização, usando a página Lambda Protection ou Accounts.

Para habilitar automaticamente o Monitoramento de atividades de rede do Lambda para novas contas-membro

1. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.

   Certifique-se de usar as credenciais da conta de GuardDuty administrador delegado.
2. Execute um destes procedimentos:
   - Usando a página Planos de Proteção:
     1. No painel de navegação, escolha Planos de proteção.
     2. Escolha Configurar todas as habilitações.
     3. Escolha Configurar contas manualmente.
     4. Selecione Habilitar automaticamente para novas contas-membro. Essa etapa garante que sempre que uma nova conta ingressar na sua organização, a Proteção do Lambda seja habilitada automaticamente para a conta dessa pessoa. Somente a

conta do GuardDuty administrador delegado da organização pode modificar essa configuração.

5. Escolha Salvar.

- Como usar a página Contas:

1. No painel de navegação, selecione Contas.
2. Na página Contas, escolha Auto-enablepreferências.
3. Na janela Gerenciar preferências de habilitação automática, selecione Habilitar para novas contas em Monitoramento de atividades de rede do Lambda.
4. Escolha Salvar.

API/CLI

Para habilitar o Lambda Network Activity Monitoring para novas contas de membros, invoque a operação da UpdateOrganizationConfigurationAPI usando a sua própria. *`detector ID`*

Como alternativa, você pode usar AWS CLI para ativar a Proteção Lambda. O exemplo a seguir mostra como você pode habilitar o Monitoramento de atividades de rede do Lambda para uma única conta de membro. *`12abc34d567e8fa901bc2d34e56789f0`*Substitua pelo ID do detector da sua conta e *`us-east-1`* pela região em que você deseja ativar a Proteção Lambda. Se não quiser habilitá-lo para todas as novas contas que ingressarem na organização, defina `AutoEnable` como `NONE`.

Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no https://console.aws.amazon.com/guardduty/console ou execute a ListDetectorsAPI.

```
aws guardduty update-organization-configuration --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --region us-east-1 --auto-enable --features
 '[{"Name": "LAMBDA_NETWORK_LOGS", "AutoEnable": "NEW"}]'
```

Quando o código é executado com êxito, ele retorna uma lista vazia de `UnprocessedAccounts`. Se houver algum problema na alteração das configurações do detector de uma conta, esse ID de conta será listado junto com um resumo do problema.

Habilite ou desabilite seletivamente o Monitoramento de atividades de rede do Lambda para contas-membro

Escolha seu método de acesso preferido para habilitar ou desabilitar seletivamente o Monitoramento de atividades de rede do Lambda para contas-membro.

Console

1. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.

   Certifique-se de usar as credenciais da conta de GuardDuty administrador delegado.

2. No painel de navegação, em Settings, selecione Accounts.

   Na página Contas, revise a coluna Monitoramento de atividades de rede do Lambda. Ele indica se o Monitoramento de atividades de rede do Lambda está habilitado ou não.

3. Escolha a conta para a qual deseja configurar a Proteção do Lambda. É possível escolher várias contas ao mesmo tempo.

4. No menu suspenso Editar planos de proteção, escolha Monitoramento de atividades de rede do Lambda e escolha uma ação apropriada.

API/CLI

Invoque a updateMemberDetectorsAPI usando a sua própria. *detector ID*

Como alternativa, você pode usar AWS CLI para ativar a Proteção Lambda. *12abc34d567e8fa901bc2d34e56789f0*Substitua pelo ID do detector da sua conta e *us-east-1* pela região em que você deseja ativar a Proteção Lambda.

Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no https://console.aws.amazon.com/guardduty/console ou execute a ListDetectorsAPI.

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --region us-east-1 --account-ids 111122223333 --features '[{"Name":
 "LAMBDA_NETWORK_LOGS", "Status": "ENABLED"}]'
```

Também é possível passar uma lista de IDs de conta separados por um espaço.

Quando o código é executado com êxito, ele retorna uma lista vazia de `UnprocessedAccounts`. Se houver algum problema na alteração das configurações do detector de uma conta, esse ID de conta será listado junto com um resumo do problema.

Como habilitar a Proteção Lambda para uma conta autônoma

Uma conta autônoma é responsável pela decisão de ativar ou desativar um plano de proteção Conta da AWS em uma conta específica Região da AWS.

Se sua conta estiver associada a uma conta de GuardDuty administrador por meio AWS Organizations ou pelo método de convite, esta seção não se aplica à sua conta. Para obter mais informações, consulte Como habilitar a proteção Lambda em ambientes com várias contas.

Depois de ativar a Proteção Lambda, GuardDuty iniciará o monitoramento Monitoramento de atividades da rede Lambda em sua conta.

Selecione o método de acesso de sua preferência para configurar a Proteção Lambda para uma conta autônoma.

Console

1. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.
2. No painel de navegação, em Configurações, escolha Proteção do Lambda.
3. A página Proteção do Lambda mostra o status atual da sua conta. Selecione Habilitar para habilitar a Proteção Lambda em sua conta.
4. Selecione Confirmar para salvar sua seleção.

API/CLI

Execute a operação da API updateDetector usando seu próprio ID de detector regional e transmitindo o `name` do objeto `features` como `LAMBDA_NETWORK_LOGS` e `status` como `ENABLED`.

Como alternativa, você pode usar AWS CLI para ativar a Proteção Lambda. Execute o comando a seguir e *`12abc34d567e8fa901bc2d34e56789f0`* substitua pelo ID do detector da sua conta e *`us-east-1`* pela região em que você deseja ativar a Proteção Lambda.

Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no https://console.aws.amazon.com/guardduty/console ou execute a ListDetectorsAPI.

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --region us-east-1 --features [{"Name" : "LAMBDA_NETWORK_LOGS", "Status" :
 "ENABLED"}]'
```

GuardDuty Investigação (Pré-visualização)

GuardDuty A investigação fornece uma análise de AI-powered segurança de suas GuardDuty descobertas e contas. Quando você cria uma investigação, GuardDuty examina a descoberta do contexto, das atividades relacionadas dos últimos 90 dias, dos recursos afetados, da inteligência de ameaças e dos indicadores de ameaças usando gráficos de conhecimento. Cada investigação fornece uma avaliação da disposição de ameaças com pontuação de confiança, classificação da técnica MITRE ATT&CK®, evidências de apoio e recomendações acionáveis.

Cada investigação produz os seguintes insights:

- Nível de risco — Uma avaliação do risco geral: Info, Baixo, Médio, Alto ou Crítico.
- Confiança — O nível de confiança da avaliação: Desconhecido, Baixo, Médio ou Alto.
- Resumo — Uma descrição dos resultados da investigação e das principais observações.
- Detalhes da investigação — Informações adicionais e contexto relacionados à investigação.
- Ações recomendadas — Ações detalhadas, incluindo os comandos da CLI, que você pode realizar para resolver os problemas identificados.

> **Note**
>
> GuardDuty A investigação está disponível somente AWS nas seguintes 10 regiões comerciais: Leste dos EUA (Norte da Virgínia), Leste dos EUA (Ohio), Oeste dos EUA (Oregon), Canadá (Central), Europa (Frankfurt), Europa (Irlanda), Europa (Londres), Europa (Paris), Europa (Estocolmo) e Ásia-Pacífico (Tóquio).

Tipos de análise

GuardDuty A investigação apóia os seguintes três tipos de análise:

- Análise de descoberta — Analisa GuardDuty descobertas específicas quando você especifica a ID de descoberta (hexadecimal de 32 caracteres). Para uma prévia, o GuardDuty Investigation suporta todas as descobertas da Extended Threat Detection (XTD) e seleciona descobertas dos planos básico, S3 e Runtime.
- Análise da conta — Analisa a postura de ameaça de uma AWS conta quando você fornece o ID da conta de 12 dígitos AWS .

- Análise da organização — Analisa a postura de ameaça da sua organização.

Cross-Region inferência

GuardDuty A investigação utiliza o Serviço de Cross-Region Inferência (CRIS), que seleciona automaticamente o ideal Região da AWS em sua região para processar a análise da investigação e gerar o relatório da investigação. Isso maximiza os recursos computacionais disponíveis, a disponibilidade do modelo e oferece a melhor experiência ao cliente.

Seus dados permanecem armazenados somente na região de origem da solicitação de investigação. No entanto, os dados da investigação e os resultados resumidos podem ser processados fora dessa região. Todos os dados são transmitidos criptografados pela rede segura da Amazon.

GuardDuty A investigação encaminha com segurança suas solicitações de inferência para os recursos computacionais disponíveis na área geográfica de origem da solicitação, conforme mostrado na tabela a seguir.

Cross-Region roteamento de inferência

Região geográfica do compatível	GuardDuty Região	Regiões de inferência
Estados Unidos	Leste dos EUA (Norte da Virgínia)	Leste dos EUA (Norte da Virgínia), Leste dos EUA (Ohio), Oeste dos EUA (Oregon)
Estados Unidos	Leste dos EUA (Ohio)	Leste dos EUA (Norte da Virgínia), Leste dos EUA (Ohio), Oeste dos EUA (Oregon)
Estados Unidos	Oeste dos EUA (Oregon)	Leste dos EUA (Norte da Virgínia), Leste dos EUA (Ohio), Oeste dos EUA (Oregon)
Estados Unidos	Canadá (Central)	Canadá (Central), Leste dos EUA (Norte da Virgínia), Leste dos EUA (Ohio), Oeste dos EUA (Oregon)
Europa	Europa (Frankfurt)	Europa (Frankfurt), Europa (Estocolmo), Europa (Milão), Europa (Espanha), Europa (Irlanda), Europa (Paris)

Região geográfica do compatível	GuardDuty Região	Regiões de inferência
Europa	Europa (Irlanda)	Europa (Frankfurt), Europa (Estocolmo), Europa (Milão), Europa (Espanha), Europa (Irlanda), Europa (Paris)
Europa	Europa (Londres)	Europa (Frankfurt), Europa (Estocolmo), Europa (Milão), Europa (Espanha), Europa (Irlanda), Europa (Londres), Europa (Paris)
Europa	Europa (Paris)	Europa (Frankfurt), Europa (Estocolmo), Europa (Milão), Europa (Espanha), Europa (Irlanda), Europa (Paris)
Europa	Europa (Estocolmo)	Europa (Frankfurt), Europa (Estocolmo), Europa (Milão), Europa (Espanha), Europa (Irlanda), Europa (Paris)
Japão	Ásia-Pacífico (Tóquio)	Ásia-Pacífico (Tóquio), Ásia-Pacífico (Osaka)

Pré-requisitos

Antes de usar a GuardDuty Investigação, verifique se os seguintes pré-requisitos foram atendidos:

- Você deve ter um GuardDuty detector ativo no Região da AWS local em que deseja criar investigações. Para obter mais informações sobre a ativação GuardDuty, consulteComeçando com GuardDuty.
- Você deve ativar o recurso GuardDuty Investigação em seu detector.

  Console

  1. Abra o GuardDuty console.
  2. No painel de navegação, selecione Configurações.
  3. Em Investigações baseadas em IA - Pré-visualização, escolha Ativar.

API/CLI

Ligue para a UpdateDetector API e ative o `AI_ANALYST` recurso em seu detector.

```
aws guardduty update-detector \
    --detector-id 2cb3d4e5f6a7b8c9d0e1f2a3b4c5d6e7 \
    --features '[{"Name": "AI_ANALYST", "Status": "ENABLED"}]'
```

- Sua identidade do IAM deve ter as permissões necessárias para realizar ações de investigação. As seguintes ações do IAM são necessárias:
  - `guardduty:CreateInvestigation`— Necessário para criar uma nova investigação.
  - `guardduty:GetInvestigation`— Necessário para recuperar os resultados da investigação.
  - `guardduty:ListInvestigations`— Necessário para listar as investigações de um detector.

O exemplo de política do IAM a seguir concede permissão para usar todas as ações de GuardDuty investigação:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "guardduty:CreateInvestigation",
                "guardduty:GetInvestigation",
                "guardduty:ListInvestigations"
            ],
            "Resource": "arn:aws:guardduty:us-
west-2:123456789012:detector/2cb3d4e5f6a7b8c9d0e1f2a3b4c5d6e7"
        }
    ]
}
```

Modelo de acesso para contas de administrador e membro

As seguintes regras de acesso se aplicam à GuardDuty Investigação, dependendo se você usa uma conta de administrador ou uma conta de membro:

- Contas de administrador — Pode criar, obter e listar investigações para si e para suas contas de membros.
- Contas de membros — Só podem obter e listar investigações para sua própria conta. As contas dos membros não podem criar investigações e não podem acessar investigações pertencentes a outras contas ou à conta do administrador.

Criando uma investigação

Você pode criar uma investigação para analisar GuardDuty descobertas e contas em seu AWS ambiente. A investigação é executada de forma assíncrona em segundo plano. Depois de criar uma investigação, use a ID da investigação para verificar seu status e recuperar os resultados.

> **Important**
>
> Durante a versão prévia, você pode iniciar até 10 investigações por conta por dia, com um limite total de 100 investigações por conta. Investigações fracassadas não contam para essas cotas. Se você estiver usando o API/CLI, o prompt de gatilho pode ter até 2.048 caracteres.

Escolha seu método de acesso preferido para criar uma investigação.

Console

1. Abra o GuardDuty console e navegue até Investigações na navegação à esquerda.
2. Escolha Iniciar investigação.
3. Selecione um escopo de investigação:
   - Uma descoberta específica — Insira a ID da descoberta que você deseja analisar.
   - Minha conta (somente independente) — Nenhuma entrada adicional é necessária. GuardDuty analisará sua conta.
   - Uma conta específica (somente administrador) — Insira o ID da AWS conta de 12 dígitos.
   - Todas as contas na organização (somente administrador) — Nenhuma entrada adicional é necessária.
4. Escolha Iniciar investigação para iniciar a análise.

API/CLI

Execute a operação CreateInvestigation da API para iniciar uma nova investigação. Você deve fornecer a ID do detector e um aviso de gatilho que descreva o que investigar.

Para encontrar o da `detectorId` sua conta e da região atual, consulte a página Configurações no https://console.aws.amazon.com/guardduty/ console ou execute a ListDetectors API.

```
aws guardduty create-investigation \
    --detector-id 2cb3d4e5f6a7b8c9d0e1f2a3b4c5d6e7 \
    --trigger-prompt "Investigate finding 1ab2c3d4e5f6a7b8c9d0e1f2a3b4c5d6 in
 account 123456789012"
```

No comando anterior, *`detector-id`* substitua o pelo seu próprio ID de detector e *`trigger-prompt`* por uma descrição do que você deseja investigar.

Opcionalmente, você pode incluir um `--client-token` parâmetro para idempotência. Se você tentar novamente a solicitação com o mesmo token de cliente, GuardDuty retornará a investigação existente em vez de criar uma duplicata.

Resultado do exemplo:

```
{
    "InvestigationId": "a1b2c3d4-5678-90ab-cdef-ef1234567890"
}
```

Requisitos de ativação

O prompt de gatilho deve descrever o que investigar. GuardDuty determina o tipo de análise com base no conteúdo do seu prompt:

- Análise de descoberta — Inclua exatamente uma ID de descoberta (cadeia hexadecimal de 32 caracteres) no prompt. A descoberta deve existir e pertencer à conta do chamador ou à conta de um membro. Você não pode incluir vários IDs de busca em um único prompt.
- Análise da conta — Inclua exatamente um ID de AWS conta de 12 dígitos no prompt. O chamador deve ser o administrador dessa conta. Você não pode incluir vários IDs de conta em um único prompt.
- Análise da organização — Descreva uma preocupação de segurança em toda a organização em sua solicitação. A investigação analisa os sinais em toda a organização.

GuardDuty usa a IA para interpretar sua solicitação de formato livre e determinar o escopo de análise apropriado. Se você incluir um ID de busca, ele executará uma análise de busca. Se você incluir um ID de conta, ele executará a análise da conta. Se sua solicitação descreve uma preocupação de toda a organização, ela realiza uma análise da organização. Se a solicitação não corresponder a um tipo de análise específico, a investigação assumirá como padrão a análise da própria conta do chamador.

Veja a seguir exemplos de solicitações de gatilho para cada tipo de análise:

- Análise de descobertas — `"Investigate finding 1ab2c3d4e5f6a7b8c9d0e1f2a3b4c5d6 in account 123456789012"`
- Análise da conta — `"Analyze findings in account with id 123456789012"`
- Análise da organização — `"Analyze findings in my organization"`

Criação de uma investigação para uma conta de membro

Se você for uma conta de administrador, poderá criar uma investigação para uma conta de membro incluindo o ID da conta de membro no prompt de gatilho. Use o ID do detector da conta do administrador no comando. Os resultados da investigação conterão descobertas da conta de membro especificada.

```
aws guardduty create-investigation \
    --detector-id 2cb3d4e5f6a7b8c9d0e1f2a3b4c5d6e7 \
    --trigger-prompt "Analyze findings in account with id 111122223333"
```

No comando anterior, substitua o pelo ID do *detector-id* detector da sua conta de administrador. O ID da conta de 12 dígitos no prompt de gatilho identifica a conta do membro a ser investigada.

Visualizando os resultados da investigação

Depois de criar uma investigação, você pode recuperar os resultados, incluindo o resumo, os detalhes da investigação, o nível de confiança e a recomendação. Uma investigação pode ter um dos seguintes status:

- EM EXECUÇÃO — A investigação ainda está em andamento.
- CONCLUÍDA — A investigação foi concluída com sucesso e os resultados estão disponíveis.

- FALHA — A investigação encontrou um erro. Verifique o campo de erro para obter detalhes.

Escolha seu método de acesso preferido para ver os resultados da investigação.

AI-generated análises e recomendações podem conter erros ou avaliações incompletas. A revisão humana é recomendada.

Console

1. Abra o GuardDuty console e navegue até Investigações na navegação à esquerda.
2. Na tabela de investigações, encontre a investigação concluída que você deseja analisar.
3. Escolha o link do título da investigação para abrir a página de detalhes.

> **Note**
>
> Os títulos de investigação só podem ser clicados quando o status é Concluído.

API/CLI

Execute a operação GetInvestigation da API para recuperar todos os detalhes de uma investigação concluída.

Para encontrar o da `detectorId` sua conta e da região atual, consulte a página Configurações no https://console.aws.amazon.com/guardduty/ console ou execute a ListDetectors API.

```
aws guardduty get-investigation \
    --detector-id 2cb3d4e5f6a7b8c9d0e1f2a3b4c5d6e7 \
    --investigation-id a1b2c3d4-5678-90ab-cdef-ef1234567890
```

Exemplo de saída para uma investigação concluída:

```
{
    "Investigation": {
        "InvestigationId": "a1b2c3d4-5678-90ab-cdef-ef1234567890",
        "Status": "COMPLETED",
        "TriggerPrompt": "Investigate finding 1ab2c3d4e5f6a7b8c9d0e1f2a3b4c5d6 in
 account 123456789012",
```

```
        "TriggeredBy": "123456789012",
        "RiskLevel": "Critical",
        "Risk": "Detection logic is valid but no live resources are compromised.",
        "Confidence": "High",
        "Summary": "{\"keyObservations\":{\"title\":\"...\",\"narrative\":\"...\",
\"observations\":[...]},\"countermeasures\":[...],\"threatAssessment\":{...}}",
        "Cloud": {
            "Provider": "AWS",
            "Region": "us-east-1",
            "Account": "123456789012"
        },
        "Metadata": {
            "Product": {
                "Name": "Amazon GuardDuty AI Analyst",
                "Feature": "Investigation"
            },
            "Version": "1.0.0"
        },
        "StartTime": 1705319400.0,
        "EndTime": 1705319700.0
    }
}
```


O `Summary` campo contém uma string JSON com os resultados completos da investigação, incluindo observações importantes, contramedidas com comandos CLI e uma avaliação de ameaças MITRE ATT&CK®.

Interpretação dos resultados da investigação

A tabela a seguir descreve os níveis de risco que uma investigação pode retornar:

Níveis de risco de investigação

Nível de risco	Description
Informações	Descoberta informativa sem risco identificado para o meio ambiente.
Baixo	Risco menor que provavelmente não exigirá ação imediata.
Médio	Risco moderado que você deve analisar e que pode precisar de correção.

Nível de risco	Description
Alto	Risco significativo que exige investigação e remediação imediatas.
Crítico	Risco grave que requer ação imediata para evitar maiores compromet imentos.

A tabela a seguir descreve os níveis de confiança:

Níveis de confiança na investigação

Nível de confiança	Description
Desconhecido	Dados insuficientes para determinar a confiança na avaliação.
Baixo	Evidências limitadas apoiam a avaliação.
Médio	Evidências moderadas apoiam a avaliação.
Alto	Evidências fortes apoiam a avaliação.

Listando investigações

Você pode listar todas as investigações de um detector, com classificação e paginação opcionais. Isso ajuda você a analisar e rastrear o status de várias investigações.

Escolha seu método de acesso preferido para listar as investigações.

Console

1. Abra o GuardDuty console e navegue até Investigações na navegação à esquerda.
2. A tabela de investigações exibe todas as investigações do detector atual com seu status, nível de risco e registros de data e hora.

API/CLI

Execute a operação ListInvestigations da API para listar os resumos das investigações de um detector.

Para encontrar o da `detectorId` sua conta e da região atual, consulte a página Configurações no https://console.aws.amazon.com/guardduty/ console ou execute a ListDetectors API.

```
aws guardduty list-investigations \
    --detector-id 2cb3d4e5f6a7b8c9d0e1f2a3b4c5d6e7 \
    --max-results 10
```

Você pode classificar os resultados especificando um `--sort-criteria` parâmetro. O exemplo a seguir lista as investigações classificadas por hora de início em ordem decrescente:

```
aws guardduty list-investigations \
    --detector-id 2cb3d4e5f6a7b8c9d0e1f2a3b4c5d6e7 \
    --sort-criteria '{"attributeName": "START_TIME", "orderBy": "DESC"}' \
    --max-results 10
```

Os atributos de classificação disponíveis são `START_TIME` `END_TIME` `STATUS``RISK_LEVEL`,, `CONFIDENCE` e. Você pode classificar em ordem `ASC` (crescente) ou `DESC` (decrescente).

Resultado do exemplo:

```
{
    "Investigations": [
        {
            "InvestigationId": "a1b2c3d4-5678-90ab-cdef-ef1234567890",
            "Status": "COMPLETED",
            "TriggerPrompt": "Investigate finding 1ab2c3d4e5f6a7b8c9d0e1f2a3b4c5d6
 in account 123456789012",
            "RiskLevel": "Critical",
            "Confidence": "High",
            "StartTime": 1705319400.0,
            "EndTime": 1705319700.0,
            "AccountId": "123456789012"
        },
        {
            "InvestigationId": "b2c3d4e5-6789-01bc-def0-ef2345678901",
            "Status": "COMPLETED",
            "TriggerPrompt": "Analyze findings in account with id 123456789012",
            "RiskLevel": "High",
            "Confidence": "High",
            "StartTime": 1705315800.0,
            "EndTime": 1705316100.0,
            "AccountId": "123456789012"
```

```
        },
        {
            "InvestigationId": "c3d4e5f6-7890-12cd-ef01-ef3456789012",
            "Status": "COMPLETED",
            "TriggerPrompt": "Analyze findings in my organization",
            "RiskLevel": "Medium",
            "Confidence": "Medium",
            "StartTime": 1705312200.0,
            "EndTime": 1705312500.0,
            "AccountId": "123456789012"
        }
    ]
}
```

Se a resposta incluir um `NextToken` valor, passe-o em uma solicitação subsequente para recuperar a próxima página de resultados. Você pode recuperar até 50 resultados por página.

Regras de detecção personalizadas em GuardDuty

As regras de detecção personalizadas fornecem uma biblioteca de regras pré-criadas que detectam atividades que você não espera que ocorram em seu AWS ambiente. GuardDuty constrói e mantém essas regras e descreve cada uma delas usando o vocabulário estabelecido de técnicas de ameaças extraído de catálogos como MITRE ATT&CK® e o Catálogo de Técnicas de AWS Ameaças. Você ativa cada regra para a atividade que deseja detectar, no modo de execução a seco para medi-la primeiro ou no modo ao vivo para gerar descobertas.

As equipes de segurança geralmente sabem que determinadas ações não devem ocorrer em contas específicas. Uma ação como compartilhar uma AMI, excluir registros de fluxo de VPC ou fazer login sem MFA pode ser rotineira em uma conta e um sinal de comprometimento em outra. A maioria das GuardDuty descobertas identifica atividades suspeitas em qualquer ambiente. As regras de detecção personalizadas permitem que você detecte atividades suspeitas somente nas contas nas quais você não espera que elas ocorram.

As regras de detecção personalizadas usam os seguintes conceitos:

Regra

Uma detecção pré-criada que GuardDuty possui e mantém. Cada regra tem como alvo uma técnica de ameaça e define as condições que fazem com que ela corresponda.

Associação

O link entre uma regra e uma conta. Uma associação registra o modo em que a regra é executada para essa conta. Uma regra sem associação não é avaliada.

Mode

O comportamento de uma regra associada quando ela corresponde à atividade. Cada regra suporta dois modos:

- Ao vivo — GuardDuty gera uma descoberta quando a regra corresponde à atividade. O modo ao vivo não expira.
- Término seco — GuardDuty avalia a regra e emite CloudWatch métricas da Amazon, mas não gera resultados. Use a operação a seco para medir o volume do sinal antes de se comprometer com a detecção ao vivo. GuardDuty emite essas métricas somente quando a regra corresponde a um evento, portanto, uma regra que nunca corresponde não produz métricas de execução seca. A tiragem a seco expira automaticamente após 14 dias.

Configuração da organização

Uma configuração de regra que a conta do GuardDuty administrador delegado aplica às contas dos membros em uma organização. GuardDuty cria as associações individuais em cada conta de destino, incluindo contas que se juntam posteriormente. Para obter mais informações, consulte Gerenciando regras de detecção personalizadas em ambientes com várias contas.

Sinal

Uma ocorrência observada da atividade que uma regra detecta. GuardDutyagrega sinais relacionados em uma única descoberta. Para obter mais informações, consulte Encontrando agregação.

Tópicos

- Como funcionam as regras de detecção personalizadas
- Regras de detecção personalizadas disponíveis
- Gerenciando regras de detecção personalizadas
- Gerenciando regras de detecção personalizadas em ambientes com várias contas

Como funcionam as regras de detecção personalizadas

Comece pesquisando as regras GuardDuty oferecidas para identificar aquelas que detectam atividades relevantes para seu ambiente. Em seguida, associe cada regra às contas em que a atividade é inesperada. Para obter mais informações sobre como associar regras a contas, consulteGerenciando regras de detecção personalizadas.

Fontes de dados e sinais

Depois de associar uma regra, GuardDuty monitora as fontes de dados das quais a regra depende e avalia os registros de entrada para eventos correspondentes. suporta eventos AWS CloudTrail de gerenciamento e eventos de monitoramento de tempo de execução. Quando a atividade observada corresponde a uma regra, GuardDuty gera um sinal. Um sinal representa uma única ocorrência observada da atividade que a regra detecta.

Cada fonte de dados tem seus próprios requisitos:

AWS CloudTrail eventos de gerenciamento

GuardDuty analisa esses eventos em todas as contas em que GuardDuty está ativado. Nenhuma configuração adicional é necessária.

Eventos de monitoramento de tempo de execução

As regras do Runtime Monitoring avaliam o processo, o arquivo e a atividade da rede que o agente de GuardDuty segurança observa em seus recursos. Uma regra de monitoramento de tempo de execução pode corresponder à atividade somente em um recurso que atenda aos dois requisitos a seguir:

- O monitoramento de tempo de execução está habilitado para o tipo de recurso: Amazon EKS, Amazon EC2 ou Amazon ECS no Fargate. Para obter mais informações, consulte GuardDuty Monitoramento de execução.
- O agente GuardDuty de segurança é executado no recurso, igual ou superior à versão mínima do agente da regra para essa plataforma.

Cada regra do Runtime Monitoring indica a versão mínima do agente necessária em cada plataforma em que pode ser executada. Para ver esses requisitos, ligue para a GetCustomDetectionRuleoperação.

Se o agente em um recurso for mais antigo do que a versão mínima de uma regra, a regra não corresponderá à atividade nesse recurso. GuardDuty não relata um erro nesse caso, portanto, mantenha o agente atualizado sobre os recursos nos quais você ativa as regras do Runtime Monitoring. Para obter informações sobre as versões do agente, consulteGuardDuty versões de lançamento do agente de segurança.

Modos

Cada associação é executada em um dos dois modos:

- Ao vivo — GuardDuty gera uma descoberta quando a regra coincide.
- Dry run — GuardDuty emite CloudWatch métricas da Amazon que contam com que frequência a regra corresponde, mas não geram descobertas. Use a simulação para medir a frequência com que uma regra é correspondida antes que ela possa criar descobertas ou acionar respostas automatizadas. As associações de tiragem a seco expiram 14 dias após a criação, as associações ativas não expiram.

Para obter mais informações, consulte Corrida a seco e Ao vivo.

Encontrando agregação

Cada descoberta segue o formato`Tactic:Service/Technique`, por exemplo, `Persistence:IAM/AccountManipulation` ou`Persistence:Runtime/SuspiciousCommand`. A forma como os GuardDuty grupos sinalizam as descobertas depende da fonte de dados que gerou o sinal, conforme descrito na lista a seguir:

- AWS CloudTrail regras — GuardDuty agrega sinais que compartilham a mesma tática, serviço e técnica em uma única descoberta. Uma única descoberta pode conter vários sinais ao GuardDuty observar a mesma atividade repetidamente a partir do mesmo diretor.
- Regras de monitoramento de tempo de execução — GuardDuty agrega sinais que compartilham os mesmos detalhes de regras, recursos e processos em uma única descoberta. Cada descoberta abrange um recurso, como uma instância, uma tarefa ou um contêiner. Os detalhes do processo que são GuardDuty comparados dependem do tipo de descoberta. Por exemplo, as descobertas de modificação do arquivo também comparam a operação do arquivo e o usuário que executou o processo. Uma correspondência repetida atualiza a descoberta existente em vez de criar uma nova. As descobertas de regras diferentes permanecem separadas, mesmo quando as regras geram o mesmo tipo de descoberta para o mesmo recurso e processo.

Para obter mais informações sobre a estrutura e os campos da descoberta, consulteRegras de detecção personalizadas encontrando detalhes.

Campos de eventos editados

as regras e avaliam os campos que são AWS CloudTrail registrados em um evento. A redação acontece antes de. GuardDuty Um AWS serviço pode redigir o valor de um campo nos eventos que ele publica. Essa redação protege dados potencialmente confidenciais. Quando um campo é redigido, AWS CloudTrail registra que o campo estava presente, mas não registra seu valor.

O serviço que publica o evento decide quais campos ele redige. Um serviço redige um campo quando esse campo pode conter informações confidenciais. A redação se aplica ao campo, não a um valor específico. Portanto, um serviço redige um campo mesmo quando o valor em uma solicitação específica não é confidencial. Ele redige esses campos para cada solicitação, independentemente de você usar o Console de gerenciamento da AWS, a AWS CLI ou AWS um SDK.

GuardDuty não é possível avaliar um valor que não esteja no evento. Se a lógica de detecção de uma regra depender de um campo redigido, a regra não coincide. GuardDuty então não produz nenhum sinal e nenhuma descoberta, mesmo que a atividade tenha ocorrido. Uma regra não será afetada se ela inspecionar somente os campos que os serviços não editam, como o nome do evento, o AWS serviço e a identidade da chamada.

A redação também pode fazer com que uma regra corresponda a uma solicitação, mas não a outra que tenha o mesmo efeito. Quando uma operação de API aceita mais de um campo para a mesma alteração, um campo pode ser editado e outro não. A correspondência da regra, então, depende de qual campo a solicitação usou.

> **Note**
>
> As regras de detecção personalizadas são um recurso de detecção, não um registro de auditoria completo. Para confirmar se uma chamada de API específica ocorreu em sua conta, analise o evento em AWS CloudTrail. Para obter mais informações, consulte Visualização de eventos com histórico de AWS CloudTrail eventos.

Regras de detecção personalizadas disponíveis

As regras de detecção personalizadas ampliam a detecção de ameaças que GuardDuty fornece. GuardDuty oferece uma biblioteca de regras de aceitação que você pode optar por ativar com base nos riscos específicos do seu ambiente. Para obter a lista atual de regras disponíveis, use a operação ListCustomDetectionRulesda API. Para os tipos de descoberta que cada regra gera, consulteTipos de localização de regras de detecção personalizadas.

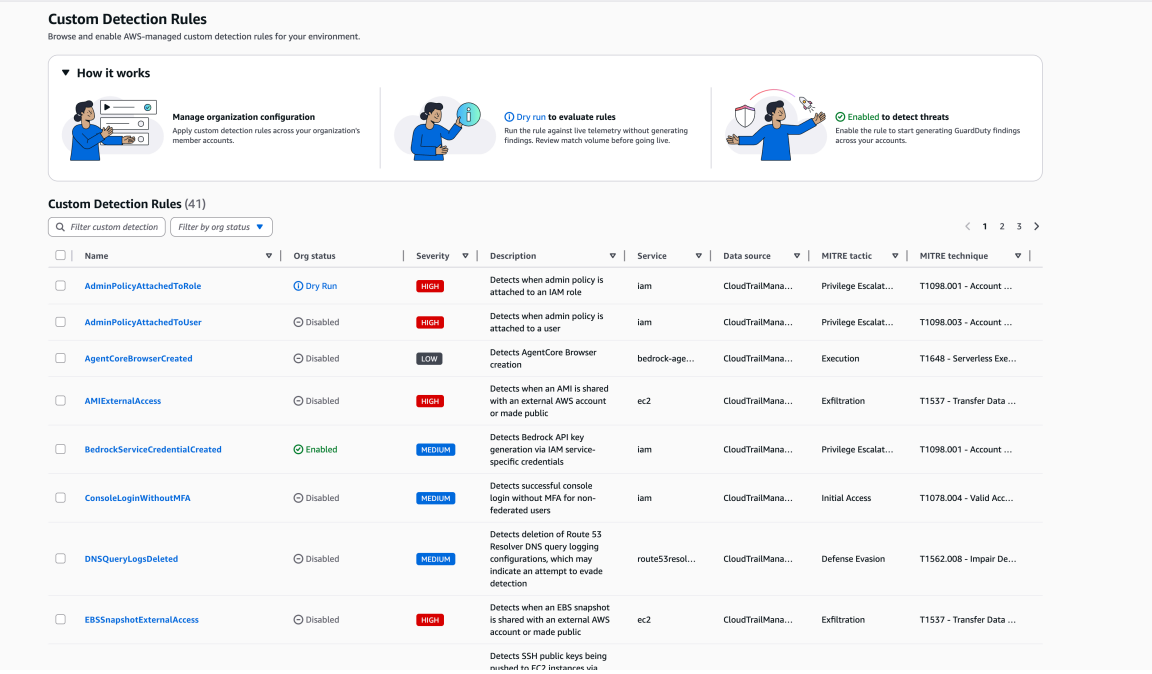
> **Note**
>
> A disponibilidade de regras individuais depende da disponibilidade do AWS serviço e do recurso correspondentes em cada região. Por exemplo, regras que têm como alvo AWS Organizations ou Amazon Simple Email Service estão disponíveis somente nas regiões em que esses serviços operam. Da mesma forma, as regras que têm como alvo URLs de funções do Lambda ou instâncias de notebooks de SageMaker IA estão disponíveis somente nas regiões em que esses recursos são compatíveis.

Visualizando a lógica de detecção de regras

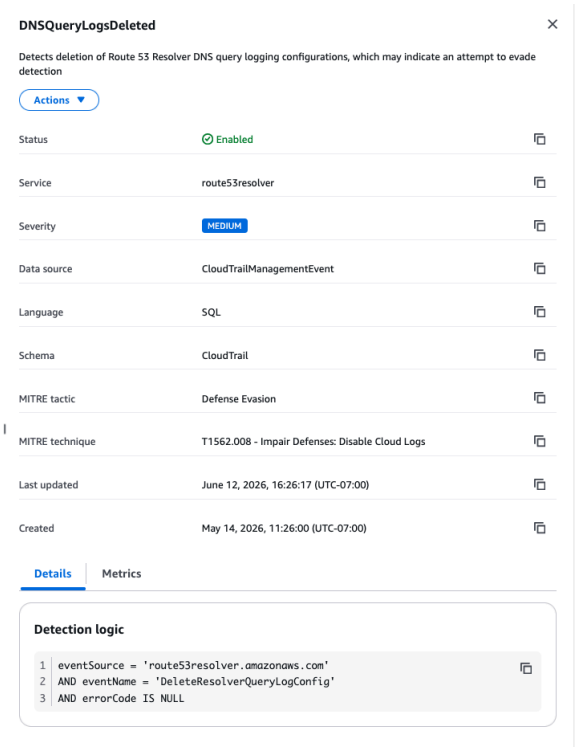
Cada regra define condições específicas que determinam quando ela é acionada. Você pode inspecionar a lógica de detecção de qualquer regra:

- Console — No GuardDuty console, navegue até Regras de Detecção Personalizadas e escolha um nome de regra. O painel dividido exibe a lógica de detecção da regra na guia Detalhes.
- API — Chame a GetCustomDetectionRuleoperação. A resposta inclui a expressão da regra no `Definition.Expression` campo.

A imagem a seguir mostra o catálogo de regras de detecção personalizadas.



A imagem a seguir mostra o painel de detalhes da regra com a lógica de detecção.



Funções usadas na lógica de detecção

As regras de detecção personalizadas usam condições SQL. AWS CloudTrail as regras avaliam campos de AWS CloudTrail eventos, e algumas usam funções especializadas para inspecionar estruturas JSON aninhadas em campos de eventos como e. `requestParameters` `responseElements` As regras do Runtime Monitoring avaliam os campos de eventos em tempo de execução, e muitas usam funções de expressão regular, principalmente para combinar as linhas de comando do processo. A tabela a seguir descreve as funções que podem aparecer na lógica de detecção de regras.

Uma regra que inspeciona um campo aninhado depende da presença desse campo no evento. Para obter mais informações sobre campos que AWS CloudTrail não registram, consulteCampos de eventos editados.

Função	Retornos	Description
`get_json_object(json, path)`	String	Extrai um valor de um documento JSON usando um caminho separado por pontos (por exemplo,) `.$.requestParameters.bucketName` Retorna o valor como uma string.

Função	Retornos	Description
`json_collect_values(json, path, field)`	Array	Navega até uma matriz em um documento JSON e coleta o campo especificado de cada elemento. Essa função extrai uma lista de valores de estruturas repetidas, como declarações de política do IAM ou regras de grupos de segurança.
`get_aws_principal(policy_json, effect)`	Array	Analisa uma política de recursos do IAM, Amazon S3 ou Lambda e retorna os principais da conta AWS a partir de declarações que correspondem ao efeito especificado (Permitir ou Negar). Essa função detecta o acesso entre contas nas políticas de recursos.
`policy_has_public_principal(policy_json, effect)`	Booleano	Retorna verdadeiro quando qualquer declaração com o efeito especificado concede acesso a um principal público (`"*"`). Essa função detecta políticas que permitem o acesso público.
`RE2_FIND(input, pattern)`	Booleano	Retorna verdadeiro quando a expressão regular RE2 `pattern` corresponde a qualquer parte de`input`. A partida diferencia maiúsculas de minúsculas. Retorna falso quando `input` é nulo. As regras de monitoramento de tempo de execução usam essa função principalmente para combinar as linhas de comando do processo.
`IRE2_FIND(input, pattern)`	Booleano	O mesmo que`RE2_FIND`, mas a partida não diferencia maiúsculas de minúsculas.

O agente GuardDuty de segurança registra os argumentos da linha de comando de um processo separados por caracteres nulos. A maioria das regras do Runtime Monitoring que correspondem a uma linha de comando primeiro substituem esses separadores por espaços, por exemplo`RE2_FIND(REPLACE(process.cmd_line, '\u0000', ' '), pattern)`.

A lógica de detecção SQL for Runtime Monitoring é uma aproximação de como GuardDuty detecta a atividade, não a lógica exata.

Gerenciando regras de detecção personalizadas

GuardDuty aplica uma regra a uma conta por meio de uma associação. Uma associação vincula uma regra à sua conta e registra o modo, ao vivo ou a seco, no qual a regra opera.

Em uma organização, a conta de GuardDuty administrador delegado usa as configurações da organização para gerenciar as regras das contas dos membros de forma centralizada. A configuração de uma organização oferece suporte à inclusão e exclusão de listas para controlar a quais contas uma regra se aplica. Para obter mais informações, consulte Gerenciando regras de detecção personalizadas em ambientes com várias contas.

Listando as regras disponíveis

O catálogo de regras lista todas as regras disponíveis, com filtros por nome, gravidade, fonte de dados, MITRE ATT&CK® tática, técnica e AWS serviço.

Console

Para listar as regras disponíveis

1. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.
2. No painel de navegação, escolha Regras de detecção personalizadas.
3. Use os controles de filtro para restringir a lista por propriedade (por exemplo, severidade ou tática).

API/CLI

Execute a ListCustomDetectionRulesoperação. Você pode passar filtros para restringir os resultados por nome, gravidade, fonte de dados, tática, técnica ou serviço.

```
aws guardduty list-custom-detection-rules \
    --filters Name=severity,Values=HIGH
```

Visualizando o status da regra

Cada regra na sua conta tem um dos três status:

- Ao vivo — A regra é associada no modo ao vivo e gera descobertas.
- Tiragem a seco — A regra está associada ao modo de execução a seco e emite somente CloudWatch métricas da Amazon.
- Desativado — A regra não tem associação e não é avaliada.

Console

A coluna Status na página Regras de Detecção Personalizadas mostra o status atual de cada regra. Você pode filtrar por status usando o menu suspenso.

API/CLI

Execute a ListCustomDetectionRuleAssociationsoperação para ver quais regras estão associadas à sua conta e seu modo atual.

```
aws guardduty list-custom-detection-rule-associations
```

Operações em massa

As operações em massa aplicam a mesma alteração de modo a mais de uma regra ou a uma regra em mais de uma conta.

Console

Na página Regras de detecção personalizadas, selecione várias regras usando as caixas de seleção e escolha Ações para ativar ou desativar todas as regras selecionadas em uma única ação.

API/CLI

Para aplicar a mesma alteração a mais de uma regra, chame CreateCustomDetectionRuleAssociationuma vez por regra.

```
for RULE in rule-id-1 rule-id-2; do
    aws guardduty create-custom-detection-rule-association \
        --rule-id "$RULE" \
```

```
        --mode LIVE
done
```

Para cobrir todas as regras do catálogo em vez de uma lista nomeada, substitua os IDs das regras pela saída de ListCustomDetectionRules:`$(aws guardduty list-custom-detection-rules --query 'Rules[].RuleId' --output text)`.

Para aplicar uma única regra a várias contas, use uma configuração de organização em vez de chamadas por conta. A configuração da organização tem como alvo as contas dos membros com listas de inclusão e exclusão e GuardDuty cria as associações individuais. Para obter mais informações, consulte Gerenciando regras de detecção personalizadas em ambientes com várias contas.

Corrida a seco

No modo de execução a seco, GuardDuty avalia os eventos de acordo com a regra, mas não gera descobertas. Em vez disso, GuardDuty emite CloudWatch métricas da Amazon que você pode usar para avaliar o volume do sinal e o comportamento das regras antes de ativar a detecção ao vivo. GuardDuty publica essas métricas somente quando a regra corresponde a um evento; se uma regra nunca corresponder, ela não produz métricas de execução seca.

Use o modo dry run para entender como uma regra se comporta em seu ambiente sem acionar respostas automatizadas ou gerar descobertas no console.

> **Note**
>
> Uma associação de tiragem seca expira 14 dias após sua criação. Quando ela expira, GuardDuty interrompe a avaliação da regra para essa conta e a regra volta a ser desativada. Para avaliar a regra novamente, crie uma nova associação de ensaio. As associações ativas não expiram.

Console

Para ativar uma regra no modo de funcionamento a seco

1. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.
2. No painel de navegação, escolha Regras de detecção personalizadas.

3. Selecione uma ou mais regras.
4. Escolha Ações e, em seguida, escolha Ativar (execução a seco).

API/CLI

Execute a CreateCustomDetectionRuleAssociationoperação com `mode` definido como`DRY_RUN`.

```
aws guardduty create-custom-detection-rule-association \
    --rule-id rule-id \
    --mode DRY_RUN
```

Ao vivo

No modo ao vivo, GuardDuty gera descobertas que aparecem no GuardDuty console. As descobertas são exportadas para a Amazon EventBridge e, se você configurar uma, para um bucket do Amazon S3 que você possui. As descobertas também são enviadas para AWS serviços integrados, como o AWS Security Hub. Use o modo ao vivo para detecção ativa de ameaças em seu ambiente.

Console

Para habilitar uma regra no modo ao vivo

1. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.
2. No painel de navegação, escolha Regras de detecção personalizadas.
3. Selecione uma ou mais regras.
4. Escolha Ações e, em seguida, escolha Ativar (ao vivo).

Para mudar uma regra existente da execução a seco para a ativa, selecione a regra, escolha Ações e, em seguida, escolha Ativar (Ao vivo).

API/CLI

Para habilitar uma nova regra no modo ao vivo, execute a CreateCustomDetectionRuleAssociationoperação com `mode` definido como`LIVE`.

```
aws guardduty create-custom-detection-rule-association \
```

```
    --rule-id rule-id \
    --mode LIVE
```

Para mudar uma regra existente da execução a seco para a ativa, execute a UpdateCustomDetectionRuleAssociationoperação.

Desativando regras

Desativar uma regra remove a associação e impede a avaliação GuardDuty de eventos em relação a essa regra para sua conta.

Console

Para desativar as regras de detecção personalizadas

1. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.
2. No painel de navegação, escolha Regras de detecção personalizadas.
3. Selecione uma ou mais regras que você deseja desativar.
4. Escolha Ações e, em seguida, escolha Desativar.
5. Confirme a ação quando solicitado.

API/CLI

Execute a DeleteCustomDetectionRuleAssociationoperação.

```
aws guardduty delete-custom-detection-rule-association \
    --rule-id rule-id
```

Gerenciando regras de detecção personalizadas em ambientes com várias contas

Em uma organização, a conta de GuardDuty administrador delegado gerencia as Regras de Detecção Personalizadas para contas de membros de forma centralizada usando as configurações da organização. O administrador declara a intenção de cada regra e a GuardDuty aplica automaticamente às contas dos membros, incluindo contas que ingressarão posteriormente.

> **Note**
>
> Multi-account o gerenciamento de Regras de Detecção Personalizadas é suportado somente para contas gerenciadas por meio de AWS Organizations. Invitation-based as contas de membros não são suportadas para o gerenciamento centralizado de regras.

Configurações da organização

Uma conta de membro não pode ativar, desativar ou alterar uma regra de detecção personalizada por si mesma. Se você tentar chamar as operações de associação de conta única a partir de uma conta membro, GuardDuty retornará um `AccessDeniedException` erro. O administrador gerencia a regra em nome do membro. Para obter mais informações sobre o administrador delegado e as contas dos membros, consulte Gerenciando várias contas em GuardDuty.

A configuração de uma organização vincula uma única regra a um conjunto de contas de membros. Ele registra o modo, ao vivo ou a seco, no qual a regra opera para essas contas. GuardDuty em seguida, cria uma associação individual para a regra em cada conta de membro alvo. Você pode configurar regras para todos os membros ou para contas específicas usando listas de inclusão e exclusão.

Console

Para configurar uma regra de detecção personalizada para a organização

1. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.
2. No painel de navegação, escolha Regras de detecção personalizadas.
3. Escolha um nome de regra para abrir os detalhes da regra e, em seguida, escolha a guia Contas.
4. Escolha Configurar ao lado de Configuração da organização.
5. Selecione o modo (Live Run ou Dry run) e escolha quais contas incluir ou excluir.

API/CLI

Crie uma configuração de organização

Execute CreateCustomDetectionRuleOrgConfigurationpara criar uma configuração de regra para contas de membros.

Atualizar a configuração de uma organização

Execute UpdateCustomDetectionRuleOrgConfigurationpara modificar o modo ou o escopo da conta.

Excluir uma configuração da organização

Execute DeleteCustomDetectionRuleOrgConfigurationpara remover a configuração da organização. Como uma regra pode conter uma configuração por modo, `mode` seleciona qual delas será removida; a outra permanece em vigor.

> **Note**
>
> A exclusão de uma configuração da organização não exclui em cascata as associações existentes de contas de membros. A regra permanece ativada nas contas dos membros onde GuardDuty já foi aplicada.

> **Note**
>
> A configuração de uma organização de execução seca expira 14 dias após sua criação. As associações de conta de membro GuardDuty criadas a partir dessa configuração expiram com ela, em vez de 14 dias após a criação de cada associação.

Executando os dois modos para a mesma regra

Uma regra contém no máximo uma configuração de organização por modo, portanto, uma regra pode ser executada no modo ativo e no modo dry run ao mesmo tempo, somente sob a seguinte condição: ambas as configurações devem nomear suas contas de destino com uma lista de inclusão explícita.

Uma configuração que afirma que toda a organização cumpre suas regras. Uma configuração reivindica toda a organização quando não nomeia nenhuma conta ou quando nomeia contas a serem excluídas. Nenhuma configuração para o outro modo pode coexistir com ele, e a tentativa de criar uma é retornada. `ConflictException` Para mover uma configuração de toda a organização para um modo diferente, atualize a configuração existente em vez de criar uma segunda.

Exemplo: aplicar uma regra no modo dry run a todas as contas dos membros

O comando da AWS CLI a seguir cria uma configuração de organização que tem como alvo todas as contas de membros, incluindo contas que ingressarão posteriormente. Omitindo ambos `--include-account-ids` e `--exclude-account-ids` tem como alvo toda a organização.

```
aws guardduty create-custom-detection-rule-org-configuration \
    --rule-id "EXAMPLE_RULE_ID" \
    --mode DRY_RUN
```

Para mover a regra para a detecção em tempo real, atualize a configuração existente com UpdateCustomDetectionRuleOrgConfiguration.

Aplicando todas as regras em uma organização

O console configura uma regra por vez. Para aplicar o mesmo modo a todas as regras disponíveis em toda a organização, faça um loop no catálogo de regras com a AWS CLI. Omitindo ambas `--include-account-ids` e `--exclude-account-ids` segmentando todas as contas de membros, incluindo contas que ingressarão posteriormente.

```
for RULE in $(aws guardduty list-custom-detection-rules \
    --query 'Rules[].RuleId' --output text); do
    aws guardduty create-custom-detection-rule-org-configuration \
        --rule-id "$RULE" \
        --mode DRY_RUN
done
```

Esse loop é usado `--mode DRY_RUN` para que você possa medir o volume do sinal antes que qualquer regra gere descobertas. Como o loop não nomeia contas, cada configuração reivindica toda a organização e aplica sua regra de forma única. Quando estiver pronto, mova cada regra para a detecção em tempo real atualizando a configuração existente com UpdateCustomDetectionRuleOrgConfiguration. Executando o loop novamente com `--mode LIVE` retornos`ConflictException`, porque a configuração de execução a seco de toda a organização já existe.

Gerenciando várias contas na Amazon GuardDuty

Quando seu AWS ambiente tem várias contas, você pode gerenciá-las designando uma Conta da AWS como a conta de administrador. Em seguida, você pode associar o Contas da AWS múltiplo a essa conta de administrador como suas contas de membros. Com essa configuração, uma conta de GuardDuty administrador designada pode avaliar e monitorar a segurança geral da sua organização. A conta do administrador também pode realizar tarefas de gerenciamento da conta, como revisar todas as descobertas geradas e configurar os planos de proteção nela. GuardDuty

Em GuardDuty, uma organização consiste em uma conta de GuardDuty administrador delegado e uma ou mais contas de membros associadas. Você pode associar as contas de duas maneiras: integrando ou usando um método antigo de enviar e aceitar convites de associação no console. AWS Organizations GuardDuty GuardDuty recomenda que você se integre com AWS Organizations o.

> **Note**
>
> O botão Editar na seção de ativação automática na página Contas redireciona você para a Configurando planos de proteção página em vez de abrir o modal de configuração antigo.

AWS Organizations é um serviço global de gerenciamento de contas que permite AWS aos administradores consolidar e gerenciar centralmente várias. Contas da AWS Ele fornece os atributos de faturamento consolidado e gerenciamento de contas, projetados para atender às necessidades orçamentárias, de segurança e de conformidade. É oferecido sem custo adicional e se integra a vários Serviços da AWS, incluindo Macie e Amazon. AWS Security Hub CSPM GuardDuty Para obter mais informações, consulte o Guia do usuário do AWS Organizations.

Conteúdo

- Entendendo a relação entre a conta GuardDuty do administrador e as contas dos membros
- Gerenciando GuardDuty contas com AWS Organizations
- Gerenciando contas usando as políticas da organização
- Gerenciando GuardDuty contas por convite
- GuardDuty considerações para exportar detalhes da conta do membro no formato CSV

Entendendo a relação entre a conta GuardDuty do administrador e as contas dos membros

Quando você usa GuardDuty em um ambiente de várias contas, a conta do administrador pode gerenciar certos aspectos GuardDuty em nome das contas dos membros. Uma conta de administrador pode executar as seguintes funções primárias:

- Adicionar e remover contas de membros associadas — O processo pelo qual uma conta de administrador pode fazer isso difere com base em como você gerencia as contas — por meio AWS Organizations ou pelo método de GuardDuty convite.

  GuardDuty recomenda gerenciar suas contas de membros por meio de AWS Organizations.
- Ativação de conta de GuardDuty administrador delegado GuardDuty na conta de gerenciamento — Se a conta AWS Organizations de gerenciamento alguma vez for desativada GuardDuty, a conta de GuardDuty administrador delegado poderá ser ativada GuardDuty na conta de gerenciamento. No entanto, é necessário que a conta de gerenciamento não tenha excluído explicitamente o Service-linked permissões de função para GuardDuty.
- Configurar o status das contas dos membros — Uma conta de administrador pode ativar ou desativar o status dos planos de GuardDuty proteção e ativar, suspender ou desativar o status de GuardDuty em nome das contas associadas dos membros.

  A conta de GuardDuty administrador delegado gerenciada com AWS Organizations pode ser ativada automaticamente GuardDuty quando Contas da AWS eles são adicionados como membros.
- Personalize quando gerar descobertas — Uma conta de administrador pode personalizar as descobertas na GuardDuty rede criando e gerenciando regras de supressão, listas de IP confiáveis e listas de ameaças. Em um ambiente de várias contas, o suporte para configurar esses recursos está disponível somente para uma conta de administrador delegado GuardDuty . Uma conta-membro não pode modificar essa configuração.

A tabela a seguir detalha a relação entre a conta GuardDuty do administrador e as contas dos membros.

Pontos chave da tabela

- Próprio: a conta só pode realizar a ação em sua própria conta.
- Qualquer — Uma conta pode realizar a ação listada para qualquer conta associada.

- Todas — Uma conta pode realizar a ação listada e ela se aplica a todas as contas associadas. Normalmente, a conta que executa essa ação é uma conta de GuardDuty administrador designada
- As células com traços (—) — As células da tabela com traços (—) indicam que a conta não pode realizar a ação listada.

Ação	Através AWS Organizations		Por convite	
	Conta de GuardDuty administrador delegada	Conta de membro associada	GuardDuty conta de administrador	Conta de membro associada
Habilitar GuardDuty	Any	–	Self	Self
Ativar GuardDuty automaticamente para toda a organização (`ALL`,`NEW`,`NONE`)	Todos	–	–	–
Visualize todas as contas dos membros da Organizations, independentemente do GuardDuty status	Any	–	–	–
Gere amostras de descobertas	Self	Self	Self	Self
Veja todas as GuardDuty descobertas	Any	Self	Any	Self

Arquive GuardDuty as descobertas	Any	–	Any	–
Aplicar regras de supressão	Todos	–	Todos	–
Crie uma lista de IPs confiáveis ou listas de ameaças	Todos	–	Todos	–
Atualizar lista de IPs confiáveis ou listas de ameaças	Todos	–	Todos	–
Excluir lista de IPs confiáveis ou listas de ameaças	Todos	–	Todos	–
Definir frequência EventBridge de notificação	Todos	–	Todos	–
Definir o local do Amazon S3 para exportar descobertas	Todos	Self	Self	Self

Habilite um ou mais planos de proteção opcionais para toda a organização (`ALL`, `NEW`, `NONE`) Isso não inclui a Proteção contra malware para o S3.	Todos	–	–	–
Ative qualquer plano de GuardDuty proteção para contas individuais Isso não inclui Proteção contra malware para o EC2 e Proteção contra malware para o S3.	Any	–	Any	–
Proteção contra malware para o EC2	Any	–	Self	–
Proteção contra malware para EC2 — verificação de On-demand malware	Any	Self	Self	Self

Proteção contra malware para S3	–	Self	–	Self
Desassociar uma conta de membro	Qualquer [+]	–	Any	–
Desassociar de uma conta de administrador	–	–	–	Self
Excluir uma conta de membro desassociada	Any	–	Any	–
Suspender GuardDuty	Qualquer [*]	–	Qualquer [*]	–
Desativar GuardDuty	Qualquer [*]	–	Qualquer [*]	Self

[+] Indica que a conta do GuardDuty administrador delegado pode realizar essa ação somente se não tiver configurado as preferências de ativação automática para `ALL` os membros da organização.

[*] Indica que uma conta de GuardDuty administrador delegado não pode ser desativada diretamente GuardDuty em uma conta de membro. A conta de GuardDuty administrador delegado deve primeiro desassociar a conta do membro e depois excluí-la. Depois disso, cada conta de membro pode ser GuardDuty desativada em suas próprias contas. Para obter mais informações sobre como executar essas tarefas na sua organização, consulte Gerenciando continuamente suas contas de membros em GuardDuty.

Entendendo o status do relacionamento dos membros

GuardDuty Operações de API, como ListMembersGetMembersretornam um `relationshipStatus` campo para cada conta de membro. Esse campo indica o estado atual do relacionamento entre a conta do administrador e a conta do membro. Verifique esse valor quando quiser confirmar que GuardDuty está monitorando ativamente a conta de um membro. Também ajuda a solucionar

o motivo pelo qual uma conta de membro não concluiu a integração ou não está mais sendo monitorada. A lista a seguir descreve os valores possíveis.

`Created`

A conta do administrador adicionou essa conta como membro (por exemplo, ligandoCreateMembers), mas o relacionamento com o membro ainda não está ativo.

`Invited`

A conta do administrador enviou um convite para essa conta de membro e o convite está aguardando para ser aceito.

`Enabled`

Essa conta de membro está associada à conta do administrador e GuardDuty está monitorando ativamente a conta do membro.

`Disabled`

Essa conta de membro está associada à conta de administrador, mas GuardDuty não está monitorando ativamente a conta de membro.

`Removed`

Essa conta de membro não está mais associada à conta do administrador. Esse status normalmente indica que a conta do administrador removeu a associação.

`Resigned`

Essa conta de membro não está mais associada à conta do administrador. Esse status normalmente indica que a conta do membro se retirou da associação.

`Deleted`

Essa conta de membro não existe mais em GuardDuty.

`EmailVerificationInProgress`

O convite desta conta de membro está pendente de verificação do endereço de e-mail.

`EmailVerificationFailed`

O convite dessa conta de membro não foi aprovado na verificação do endereço de e-mail.

`RegionDisabled`

Essa conta de membro não pode ser monitorada porque GuardDuty não está ativada ou não está disponível no momento Região da AWS.

`AccountSuspended`

Este membro Conta da AWS está em estado suspenso.

`CannotCreateDetectorInOrganizationMasterAccount`

GuardDuty não é possível criar um detector na conta AWS Organizations de gerenciamento, normalmente porque as permissões necessárias da função vinculada ao serviço estão ausentes.

Gerenciando GuardDuty contas com AWS Organizations

Em uma AWS organização, a conta de gerenciamento pode designar qualquer conta dentro dessa organização como a conta de GuardDuty administrador delegado. Para essa conta de administrador, GuardDuty é ativada automaticamente somente na conta atual Região da AWS. Por padrão, a conta de administrador pode ativar e gerenciar GuardDuty todas as contas de membros na organização dentro dessa região. A conta do administrador pode visualizar e adicionar membros a essa AWS organização.

As seções a seguir o guiarão por várias tarefas que você pode realizar como uma conta de GuardDuty administrador delegado.

Conteúdo

- Considerações e recomendações para uso com GuardDuty AWS Organizations
- Permissões necessárias para designar uma conta de administrador delegado GuardDuty
- Designação de uma conta de administrador delegado GuardDuty
- Como configurar as preferências de habilitação automática da organização
- Como adicionar membros à organização
- (Opcional) Ativar planos de proteção para contas-membro existentes
- Gerenciando continuamente suas contas de membros em GuardDuty
- Suspensão da GuardDuty conta de membro
- Como desassociar (remover) a conta-membro da conta de administrador
- Excluindo contas de membros da organização GuardDuty
- Alterando a conta do GuardDuty administrador delegado

Considerações e recomendações para uso com GuardDuty AWS Organizations

As considerações e recomendações a seguir podem ajudá-lo a entender como uma conta de GuardDuty administrador delegado opera em: GuardDuty

Uma conta de GuardDuty administrador delegado pode gerenciar no máximo 50.000 membros.

> Há um limite de 50.000 contas de membros por conta de GuardDuty administrador delegado. Isso inclui contas de membros que foram adicionadas por meio de AWS Organizations ou aquelas que aceitaram o convite da conta de GuardDuty administrador para ingressar na organização. No entanto, pode haver mais de 50.000 contas em sua AWS organização.
>
> Se você exceder o limite de 50.000 contas de membros, receberá uma notificação e um e-mail para a conta de CloudWatch GuardDuty administrador delegado designada. Health Dashboard

Uma conta de GuardDuty administrador delegado é regional.

> Ao contrário AWS Organizations, GuardDuty é um serviço regional. As contas de GuardDuty administrador delegado e suas contas de membros devem ser adicionadas AWS Organizations em cada região desejada em que você GuardDuty ativou. Se a conta de gerenciamento da organização designar uma conta de GuardDuty administrador delegado somente no Leste dos EUA (Norte da Virgínia), a conta de GuardDuty administrador delegado gerenciará somente as contas de membros adicionadas à organização nessa região. Para obter mais informações sobre a paridade de recursos nas regiões onde GuardDuty está disponível, consulteRegiões e endpoints.

Casos especiais para regiões de inclusão

- Quando uma conta de GuardDuty administrador delegado opta por não participar de uma região opcional, mesmo que sua organização tenha a configuração de ativação GuardDuty automática definida apenas para novas contas de membros (`NEW`) ou para todas as contas de membros (`ALL`), GuardDuty não pode ser habilitada para nenhuma conta membro na organização que esteja atualmente desativada. GuardDuty Para obter informações sobre a configuração de suas contas de membros, abra Contas no painel de navegação do GuardDuty console ou use a ListMembersAPI.
- Ao trabalhar com a configuração de GuardDuty ativação automática definida como`NEW`, certifique-se de que a seguinte sequência seja atendida:

  1. As contas-membro aderem a uma região de inclusão.

2. Adicione as contas-membro à sua organização em AWS Organizations.

Se você alterar a ordem dessas etapas, a configuração de GuardDuty ativação automática não **NEW** funcionará na região de inscrição específica porque a conta do membro não é mais nova na organização. GuardDuty fornece duas soluções alternativas:

- Defina a configuração de GuardDuty ativação automática comoALL, que inclui contas de membros novas e existentes. Nesse caso, a ordem das etapas é irrelevante.
- Se uma conta de membro já fizer parte da sua organização, gerencie a GuardDuty configuração dessa conta individualmente na região de inscrição específica usando o GuardDuty console ou a API.

Necessário para que uma AWS organização tenha a mesma conta de GuardDuty administrador delegado em todos os Regiões da AWS.

Você deve designar uma conta de membro como a conta de GuardDuty administrador delegado em todos os Regiões da AWS lugares GuardDuty ativados. Por exemplo, se você designar uma conta de membro *111122223333* em*Europe (Ireland)*, não poderá designar outra conta de membro em*555555555555*. *Canada (Central)* É necessário que você use a mesma conta da conta de GuardDuty administrador delegado em todas as outras regiões.

Você pode designar uma nova conta de GuardDuty administrador delegado a qualquer momento. Para obter mais informações sobre como remover a conta de GuardDuty administrador delegado existente, consulteAlterando a conta do GuardDuty administrador delegado.

Não é recomendável definir a conta de gerenciamento da sua organização como a conta de GuardDuty administrador delegado.

A conta de gerenciamento da sua organização pode ser a conta de GuardDuty administrador delegado. No entanto, as práticas recomendadas de segurança da AWS seguem o princípio do privilégio mínimo e não recomendam essa configuração.

Alterar uma conta de GuardDuty administrador delegado não desativa GuardDuty as contas dos membros.

Se você remover uma conta de GuardDuty administrador delegado, GuardDuty removerá todas as contas de membros associadas a essa conta de GuardDuty administrador delegado. GuardDuty ainda permanece habilitado para todas essas contas de membros.

Permissões necessárias para designar uma conta de administrador delegado GuardDuty

Para começar a usar a Amazon GuardDuty com AWS Organizations, a conta AWS Organizations de gerenciamento da organização designa uma conta como a conta de GuardDuty administrador delegado. Isso permite GuardDuty , como um serviço confiável, em AWS Organizations. Também habilita GuardDuty a conta de GuardDuty administrador delegado e também permite que a conta de administrador delegado habilite e GuardDuty gerencie outras contas na organização na região atual. Para obter informações sobre como essas permissões são concedidas, consulte Usando AWS Organizations com outros AWS serviços.

Como conta de AWS Organizations gerenciamento, antes de designar a conta de GuardDuty administrador delegado para sua organização, verifique se você pode realizar a seguinte GuardDuty ação:. `guardduty:EnableOrganizationAdminAccount` Essa ação permite que você designe a conta de GuardDuty administrador delegado para sua organização usando. GuardDuty Você também deve garantir que tenha permissão para realizar as AWS Organizations ações que ajudam a recuperar informações sobre sua organização.

Para conceder essas permissões, inclua a seguinte declaração em uma política AWS Identity and Access Management (IAM) da sua conta:

```
{
    "Sid": "PermissionsForGuardDutyAdmin",
    "Effect": "Allow",
    "Action": [
        "guardduty:EnableOrganizationAdminAccount",
        "organizations:EnableAWSServiceAccess",
        "organizations:RegisterDelegatedAdministrator",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListRoots"
    ],
    "Resource": "*"
}
```

Se você quiser designar sua conta AWS Organizations de gerenciamento como conta de GuardDuty administrador delegado, sua conta também precisará da ação IAM:. `CreateServiceLinkedRole` Essa ação permite que você inicialize GuardDuty para a conta de gerenciamento. No entanto, revise Considerações e recomendações para uso com GuardDuty AWS Organizations antes de prosseguir com a adição das permissões.

Para continuar a designar a conta de gerenciamento como a conta de GuardDuty administrador delegado, adicione a seguinte declaração à política do IAM e *111122223333* substitua pela Conta da AWS ID da conta de gerenciamento da sua organização:

```
{
 "Sid": "PermissionsToEnableGuardDuty"
 "Effect": "Allow",
 "Action": [
  "iam:CreateServiceLinkedRole"
 ],
 "Resource": "arn:aws:iam::111122223333:role/aws-service-role/guardduty.amazonaws.com/
AWSServiceRoleForAmazonGuardDuty",
 "Condition": {
  "StringLike": {
   "iam:AWSServiceName": "guardduty.amazonaws.com"
  }
 }
}
```

Designação de uma conta de administrador delegado GuardDuty

Esta seção apresenta as etapas para designar um administrador delegado na organização da GuardDuty.

Como conta de gerenciamento da AWS organização, leia atentamente Considerações e recomendações sobre como uma conta de GuardDuty administrador delegado opera. Antes de continuar, verifique se você tem Permissões necessárias para designar uma conta de administrador delegado GuardDuty.

Escolha um método de acesso preferencial para designar uma conta de GuardDuty administrador delegado para sua organização. Somente uma conta de gerenciamento pode executar essa etapa.

Console

1. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.

Para acessar, use as credenciais da conta de gerenciamento de sua organização da AWS Organizations .

2. Usando o Região da AWS seletor no canto superior direito da página, selecione a região na qual você deseja designar a conta de GuardDuty administrador delegado para sua organização.
3. Siga um destes procedimentos, dependendo se GuardDuty está habilitado para sua conta de gerenciamento na região atual:

   - Se não GuardDuty estiver ativado, selecione Amazon GuardDuty - todos os recursos e escolha Começar. Essa ação levará você à GuardDuty página Bem-vindo ao.
   - Se GuardDuty estiver ativado, escolha Configurações no painel de navegação.
4. Em Administrador delegado, insira a Conta da AWS ID de 12 dígitos da conta que você deseja designar como a conta de GuardDuty administrador delegado da organização.
5. Selecione Delegar.
6. (Recomendado) Repita as etapas anteriores para designar a conta de GuardDuty administrador delegado em cada uma Região da AWS onde você ativou. GuardDuty

API/CLI

1. Execute enableOrganizationAdminAccountusando as credenciais da conta Conta da AWS de gerenciamento da organização.

   - Como alternativa, você pode usar AWS Command Line Interface para fazer isso. O AWS CLI comando a seguir designa uma conta de GuardDuty administrador delegado somente para sua região atual. Execute o AWS CLI comando a seguir e certifique-se de *111111111111* substituir pela Conta da AWS ID da conta que você deseja designar como conta de GuardDuty administrador delegado:

     ```
     aws guardduty enable-organization-admin-account --admin-account-
     id 111111111111
     ```

     Para designar a conta de GuardDuty administrador delegado para outras regiões, especifique a região no AWS CLI comando. O exemplo a seguir demonstra como habilitar uma conta de GuardDuty administrador delegado no Oeste dos EUA (Oregon). Certifique-se de *us-west-2* substituir pela região à qual você deseja atribuir a conta de GuardDuty administrador delegado.

```
aws guardduty enable-organization-admin-account --admin-account-
id 111111111111 --region us-west-2
```

Para obter informações sobre Regiões da AWS onde GuardDuty está disponível, consulteRegiões e endpoints.

Se GuardDuty estiver desativado para sua conta de GuardDuty administrador delegado, não será possível realizar nenhuma ação. Se ainda não tiver feito isso, certifique-se de habilitar a conta GuardDuty de GuardDuty administrador delegado recém-designada.

2. (Recomendado) repita as etapas anteriores para designar a conta de GuardDuty administrador delegado em cada uma Região da AWS onde você ativou. GuardDuty

Como configurar as preferências de habilitação automática da organização

O recurso de ativação automática da organização GuardDuty ajuda você a definir o mesmo GuardDuty status dos planos de proteção para contas `ALL` existentes ou `NEW` membros em sua organização, em uma única etapa. Da mesma forma, é possível especificar quando não se deseja realizar nenhuma ação nas contas de membros, selecionando `NONE`. As etapas a seguir explicam essas configurações e também indicam quando é necessário usar uma configuração específica.

> **Note**
>
> Você pode definir preferências de habilitação automática para todos os planos de proteção, exceto Proteção contra malware para S3.

Selecione um método de acesso preferencial para atualizar as preferências de habilitação automática da organização.

Console

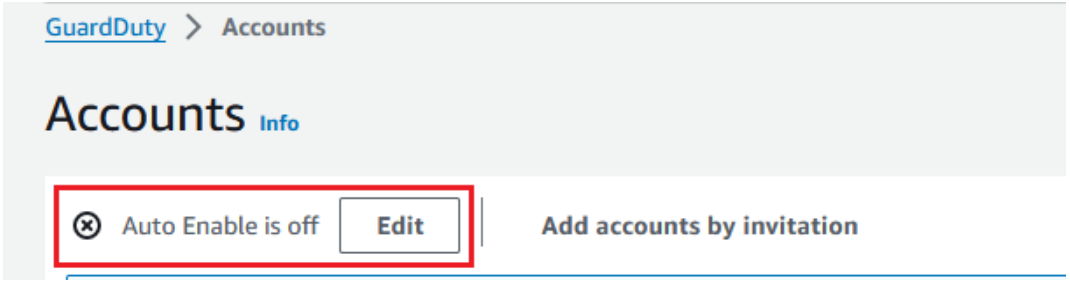
1. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.

   Para entrar, use as credenciais da conta de GuardDuty administrador.

2. No painel de navegação, selecione Contas.

A página Contas fornece opções de configuração para a conta do GuardDuty administrador Auto-enable GuardDuty e os planos de proteção opcionais em nome das contas membros que pertencem à organização.

3. Para atualizar as configurações de habilitação automática em vigor, selecione Editar.



Esse suporte está disponível para configuração GuardDuty e para todos os planos de proteção opcionais compatíveis em seu Região da AWS. Você pode selecionar uma das seguintes opções de configuração GuardDuty em nome de suas contas de membros:

- Habilitar para todas as contas (**`ALL`**): selecionar para habilitar a respectiva opção para todas as contas em uma organização. Isso inclui novas contas que ingressam na organização e aquelas contas que podem ter sido suspensas ou removidas da organização. Isso também inclui a conta de GuardDuty administrador delegado.

  > **Note**
  >
  > Pode levar até 24 horas para atualizar a configuração de todas as contas-membro.

- Auto-enable para novas contas (**`NEW`**) — Selecione para ativar GuardDuty ou ativar os planos de proteção opcionais somente para novas contas de membros automaticamente quando elas ingressarem na sua organização.
- Não habilitar (**`NONE`**): selecionar para impedir a habilitação da respectiva opção para novas contas em sua organização. Nesse caso, a conta GuardDuty do administrador gerenciará cada conta individualmente.

  Ao atualizar a configuração de habilitar automática de `ALL` ou `NEW` para `NONE`, essa ação não desabilita a respectiva opção para suas contas existentes. Essa configuração será aplicada às novas contas que ingressam na organização. Depois de atualizar as configurações de habilitação automática, nenhuma nova conta terá a respectiva opção habilitada.

> **Note**
>
> Quando uma conta de GuardDuty administrador delegado opta por não participar de uma região opcional, mesmo que sua organização tenha a configuração de ativação GuardDuty automática definida apenas para novas contas de membros (`NEW`) ou para todas as contas de membros (`ALL`), GuardDuty não pode ser habilitada para nenhuma conta membro na organização que esteja atualmente desativada. GuardDuty Para obter informações sobre a configuração de suas contas de membros, abra Contas no painel de navegação do GuardDuty console ou use a ListMembersAPI.

4. Escolha Salvar alterações.
5. (Opcional) caso queira usar as mesmas preferências em cada região, atualize suas preferências em cada uma das regiões atendidas separadamente.

   Alguns dos planos de proteção opcionais podem não estar disponíveis em todos os Regiões da AWS lugares GuardDuty disponíveis. Para obter mais informações, consulte Regiões e endpoints.

API/CLI

1. Execute UpdateOrganizationConfigurationusando as credenciais da conta de GuardDuty administrador delegado, para configurar automaticamente planos GuardDuty de proteção opcionais nessa região para sua organização. Para obter informações sobre as várias configurações de ativação automática, consulte auto. EnableOrganizationMembers

   Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no https://console.aws.amazon.com/guardduty/console ou execute a ListDetectorsAPI.

   Para definir preferências de habilitação automática para qualquer um dos planos de proteção opcionais compatíveis em sua região, siga as etapas fornecidas nas seções de documentação correspondentes de cada plano de proteção.
2. Você pode validar as preferências da sua organização na região atual. Executar describeOrganizationConfiguration. Certifique-se de especificar o ID do detector da conta do GuardDuty administrador delegado.

> **Note**
>
> Pode levar até 24 horas para atualizar a configuração de todas as contas-membro.

3. Como alternativa, execute o AWS CLI comando a seguir para definir as preferências a serem ativadas ou desativadas automaticamente GuardDuty nessa região para novas contas (`NEW`) que ingressam na organização, todas as contas (`ALL`) ou nenhuma das contas (`NONE`) na organização. Para obter mais informações, consulte auto EnableOrganizationMembers. Com base na sua preferência, talvez seja necessário substituir `NEW` por `ALL` ou `NONE`. Se você configurar o plano de proteção com`ALL`, o plano de proteção também será habilitado para a conta de GuardDuty administrador delegado. Certifique-se de especificar o ID do detector da conta do GuardDuty administrador delegado que gerencia a configuração da organização.

   Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no https://console.aws.amazon.com/guardduty/console ou execute a ListDetectorsAPI.

   ```
   aws guardduty update-organization-configuration --detector-
   id 12abc34d567e8fa901bc2d34e56789f0 --auto-enable-organization-members=NEW
   ```

4. É possível validar as preferências da sua organização na região atual. Execute o AWS CLI comando a seguir usando o ID do detector da conta do GuardDuty administrador delegado.

   ```
   aws guardduty describe-organization-configuration --detector-
   id 12abc34d567e8fa901bc2d34e56789f0
   ```

(Recomendado) repita as etapas anteriores em cada região usando o ID delegado do detector da conta de GuardDuty administrador.

> **Note**
>
> Quando uma conta de GuardDuty administrador delegado opta por não participar de uma região opcional, mesmo que sua organização tenha a configuração de ativação GuardDuty automática definida apenas para novas contas de membros (`NEW`) ou para todas as contas de membros (`ALL`), GuardDuty não pode ser habilitada para nenhuma conta membro na organização que esteja atualmente desativada. GuardDuty Para obter

informações sobre a configuração de suas contas de membros, abra Contas no painel de navegação do GuardDuty console ou use a ListMembersAPI.

Como adicionar membros à organização

Como conta de GuardDuty administrador delegado, você pode adicionar uma ou mais Contas da AWS à GuardDuty organização. Quando você adiciona uma conta como GuardDuty membro, ela será GuardDuty ativada automaticamente nessa região. Há uma exceção na conta de gerenciamento da organização. Antes que a conta de gerenciamento seja adicionada como GuardDuty membro, ela deve estar GuardDuty ativada.

Escolha um método preferido para adicionar uma conta de membro à sua GuardDuty organização.

Console

1. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.

   Para entrar, use as credenciais da conta de GuardDuty administrador delegado.
2. No painel de navegação, selecione Contas.

   A tabela de contas exibe todas as contas de membros que estão ativas (não suspensas Contas da AWS) e podem estar associadas à conta de GuardDuty administrador delegado. Caso a conta-membro esteja associada à conta de administrador da organização, o Tipo será um dos seguintes: Via organizações ou Por convite. Se uma conta de membro não estiver associada à conta de GuardDuty administrador da organização, o Tipo dessa conta de membro será Não membro.
3. Selecione um ou mais IDs de conta que deseja adicionar como membros. Esses IDs de conta devem ter o Tipo de Via Organizações.

   As contas adicionadas por meio de convite não fazem parte da sua organização. Você pode gerenciar essas contas individualmente. Para obter mais informações, consulte Gerenciar contas por convite.
4. Escolha no menu suspenso Ações e selecione Adicionar membro. Depois de adicionar essa conta como membro, a GuardDuty configuração de ativação automática será aplicada. Com base nas configurações emComo configurar as preferências de habilitação automática da organização, a GuardDuty configuração dessas contas pode mudar.

5. Você pode selecionar a seta para baixo da coluna Status para classificar as contas pelo status Não é membro e, em seguida, escolher cada conta que não GuardDuty esteja ativada na região atual.

   Se nenhuma das contas listadas na tabela de contas ainda tiver sido adicionada como membro, você poderá habilitar GuardDuty na região atual todas as contas da organização. Escolha a opção para habilitar na faixa na parte superior da página. Essa ação ativa automaticamente a Auto-enable GuardDuty configuração para que GuardDuty seja habilitada para qualquer nova conta que ingresse na organização.

6. Selecione Confirmar para adicionar as contas como membros. Essa ação também é GuardDuty ativada para todas as contas selecionadas. O Status das contas convidadas será alterado para Habilitado.

7. (Recomendado) Repita essas etapas em cada uma Região da AWS. Isso garante que a conta de GuardDuty administrador delegado possa gerenciar descobertas e outras configurações para contas de membros em todas as regiões em que GuardDuty você habilitou.

   O recurso de ativação automática habilita GuardDuty para todos os futuros membros de sua organização. Isso permite que sua conta de GuardDuty administrador delegado gerencie quaisquer novos membros criados ou adicionados à organização. Quando o número de contas de membros atinge o limite de 50.000, o Auto-enable recurso é automaticamente desativado. Se você remover uma conta de membro e o número total de membros diminuir para menos de 50.000, o Auto-enable recurso será ativado novamente.

API/CLI

- Execute CreateMembersusando as credenciais da conta de GuardDuty administrador delegado.

  Você deve especificar o ID do detector regional da conta do GuardDuty administrador delegado e os detalhes da conta (Conta da AWS IDs e endereços de e-mail correspondentes) das contas que você deseja adicionar como GuardDuty membros. É possível criar um ou mais membros com essa operação de API.

  Ao executar CreateMembers na sua organização, as preferências de habilitação automática para novos membros serão aplicadas à medida que novas contas de membros ingressarem na sua organização. Ao executar CreateMembers com uma conta-membro existente, a

configuração da organização também se aplicará aos membros existentes. Isso pode alterar a configuração atual das contas-membro antigas.

Execute ListAccountsna Referência AWS Organizations da API para ver todas as contas na AWS organização.

- Como alternativa, você pode usar AWS Command Line Interface. Execute o comando AWS CLI a seguir e certifique-se de usar seu próprio ID de detector válido, ID de Conta da AWS e endereço de e-mail associado ao ID da conta.

  Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no https://console.aws.amazon.com/guardduty/console ou execute a ListDetectorsAPI.

  ```
  aws guardduty create-members --detector-id 12abc34d567e8fa901bc2d34e56789f0
   --account-details AccountId=111122223333,Email=guardduty-member-
  name@amazon.com
  ```

  Você pode ver uma lista de todos os integrantes da organização executando o seguinte AWS CLI comando:

  ```
  aws organizations list-accounts
  ```

Depois de adicionar essa conta como membro, a GuardDuty configuração de ativação automática será aplicada.

(Opcional) Ativar planos de proteção para contas-membro existentes

O procedimento a seguir inclui etapas para habilitar planos de proteção para contas-membro existentes usando a página Contas. Para ver as etapas para fazer isso usando a API ou AWS CLI consulte os documentos relacionados ao plano de proteção específico.

Pode-se habilitar planos de proteção para contas individuais na página Contas.

1. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.

   Use as credenciais da conta de GuardDuty administrador delegado.

2. No painel de navegação, selecione Contas.

3. Selecione uma ou mais contas para as quais você deseja configurar um plano de proteção. Repita as etapas a seguir para cada plano de proteção que você deseja configurar:

   a. Selecione Editar planos de proteção.
   b. Na lista de planos de proteção, escolha um plano de proteção que deseja configurar.
   c. Selecione uma das ações que você deseja realizar para esse plano de proteção e, em seguida, selecione Confirmar.
   d. Para a conta selecionada, a coluna correspondente ao plano de proteção configurado mostrará a configuração atualizada como Habilitada ou Não habilitada.

Gerenciando continuamente suas contas de membros em GuardDuty

Como conta de GuardDuty administrador delegado, você é responsável por manter a configuração GuardDuty e seus planos de proteção opcionais para todas as contas da sua organização em cada uma das contas suportadas Região da AWS. As seções a seguir fornecem as opções para manter o status da configuração GuardDuty ou de qualquer um de seus planos de proteção opcionais:

Para manter o status de configuração de toda a sua organização em cada região

- Defina preferências de ativação automática para toda a organização usando o GuardDuty console — Você pode habilitar GuardDuty automaticamente para todos (`ALL`) os membros da organização ou para os novos (`NEW`) membros que ingressam na organização, ou optar por não (`NONE`) ativá-la automaticamente para nenhum dos membros da organização.

  Você também pode definir as mesmas configurações ou configurações diferentes para qualquer um dos planos de proteção incluídos GuardDuty.

  Pode levar até 24 horas para atualizar a configuração de todas as contas-membro da organização.
- Atualize as preferências de ativação automática usando a API — Execute UpdateOrganizationConfigurationpara configurar automaticamente GuardDuty e seus planos de proteção opcionais para a organização. Quando você corre CreateMemberspara adicionar novas contas de membros em sua organização, as configurações definidas serão aplicadas automaticamente. Ao executar CreateMembers com uma conta-membro existente, a configuração da organização também se aplica aos membros existentes. Isso pode alterar a configuração atual das contas-membro antigas.

  Para ver todas as contas em sua organização, execute ListAccountsna Referência da AWS Organizations API.

Para manter o status de configuração das contas-membro individualmente em cada região

- Para ver todas as contas em sua organização, execute ListAccountsna Referência da AWS Organizations API.
- Quando você quiser que contas de membros seletivas tenham um status de configuração diferente, execute UpdateMemberDetectorspara cada conta de membro individualmente.

  Você pode usar o GuardDuty console para realizar a mesma tarefa navegando até a página Contas no GuardDuty console.

  Para obter informações sobre como habilitar planos de proteção para contas individuais usando o console ou a API, consulte a página de configuração do respectivo plano de proteção.

Suspensão da GuardDuty conta de membro

Como conta de GuardDuty administrador delegado, você pode suspender o GuardDuty serviço de uma conta de membro em sua organização. Se você fizer isso, a conta do membro ainda permanecerá na sua GuardDuty organização. Você também pode reativar GuardDuty essas contas de membros posteriormente. No entanto, caso queira eventualmente desassociar (remover) essa conta-membro, depois de seguir as etapas desta seção, deve-se seguir as etapas em Como desassociar (remover) a conta-membro da conta de administrador.

Ao suspender uma conta GuardDuty de membro, você pode esperar as seguintes alterações:

- GuardDuty não monitora mais a segurança do AWS ambiente nem gera novas descobertas.
- As descobertas existentes na conta-membro permanecem intactas.
- Uma conta de membro GuardDuty suspensa não incorre em nenhuma cobrança por. GuardDuty

  Se a conta do membro tiver ativado a Proteção contra Malware para S3 para um ou mais buckets em sua conta, a suspensão GuardDuty não afetará a configuração da Proteção contra Malware para S3. A conta do membro continuará incorrendo no custo de uso da Proteção contra Malware para o S3. Para que a conta-membro pare de usar a Proteção contra Malware para o S3, ela deve desabilitar esse recurso para os buckets protegidos. Para obter mais informações, consulte Desativando a proteção contra malware para S3 em um bucket protegido.

Escolha um método preferencial para suspender GuardDuty uma conta de membro em sua organização.

Console

1. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.

   Para entrar, use as credenciais da conta de GuardDuty administrador delegado.
2. No painel de navegação, selecione Contas.
3. Na página Contas, selecione uma ou mais contas que você deseja suspender GuardDuty.
4. Escolha o menu suspenso Ações e, em seguida, escolha Suspender. GuardDuty
5. Escolha Suspender GuardDuty para confirmar a seleção.

   Isso mudará o status da conta-membro para Desativada (suspensa).

   Repita as etapas anteriores em cada região adicional em que deseja desassociar ou remover a conta-membro.

API

1. Para recuperar o ID da conta do membro que você deseja suspender GuardDuty, use a ListMembersAPI. Inclua o parâmetro `OnlyAssociated` na sua solicitação. Se você definir o valor desse parâmetro como`true`, GuardDuty retornará uma `members` matriz que fornece detalhes somente sobre as contas que atualmente são GuardDuty membros.

   Como alternativa, você pode usar AWS Command Line Interface (AWS CLI) para executar o seguinte comando:

   ```
   aws guardduty list-members --only-associated true --region us-east-1
   ```

   Substitua *`us-east-1`* pela região em que você deseja suspender GuardDuty essa conta.
2. Para suspender uma ou mais contas de GuardDuty membros, execute StopMonitoringMembers GuardDuty para suspender uma conta de membro.

   Como alternativa, você pode usar AWS CLI para executar o seguinte comando:

   ```
   aws guardduty stop-monitoring-members --detector-id
    12abc34d567e8fa901bc2d34EXAMPLE --account-ids 111122223333 --region us-east-1
   ```

   Substitua *`us-east-1`* pela região em que você deseja suspender essa conta. Caso tenha uma lista de IDs da conta que deseja remover, separe-os com um caractere de espaço.

Caso queira ainda desassociar (remover) essa conta-membro, siga as etapas em Como desassociar (remover) a conta-membro da conta de administrador.

Como desassociar (remover) a conta-membro da conta de administrador

Quando você quiser parar de definir as GuardDuty configurações e acessar os dados de uma conta de membro, remova essa conta como conta de GuardDuty membro. Você pode fazer isso desassociando (removendo) essa conta da conta de GuardDuty administrador.

Quando você desassocia uma conta de GuardDuty membro, acontece o seguinte:

- GuardDuty permanece ativada para a conta atual Região da AWS, mas a conta é desassociada da conta de GuardDuty administrador delegado.
- A conta desassociada continua sendo exibida no inventário de contas.
- A conta GuardDuty do administrador não tem mais acesso às descobertas dessa conta independente.
- O proprietário da conta não é notificado da desassociação.

Você pode adicionar a conta desassociada à sua organização de novo posteriormente.

Escolha um método de sua preferência para desassociar (remover) uma conta de associado da sua organização.

Console

1. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.

   Para entrar, use as credenciais da conta de GuardDuty administrador delegado.
2. No painel de navegação, selecione Contas.
3. Na tabela Contas, remova uma conta que tenha Tipo como Via Organizações e Status como Habilitada.

   Selecione uma ou mais contas com o mesmo Tipo e Status.
4. No menu suspenso Ações, selecione Desassociar conta.
5. Selecione Desassociar conta para confirmar sua seleção.
6. O valor do Status das contas selecionadas será alterado para Não é membro. A contagem de Via Organizations (Active/All) no canto superior direito da página Contas será alterada para refletir a atualização.

Repita as etapas anteriores em cada região adicional em que deseja desassociar a conta-membro.

API

1. Para recuperar o ID da conta-membro que deseja remover, use a API ListMembers. Inclua o `OnlyAssociated` parâmetro na solicitação. Se você definir o valor desse parâmetro como`true`, GuardDuty retornará uma `members` matriz que fornece detalhes somente sobre as contas que atualmente são GuardDuty membros.

   Como alternativa, você pode usar AWS Command Line Interface (AWS CLI) para executar o seguinte comando:

   ```
   aws guardduty list-members --only-associated true --region us-east-1
   ```

   Substitua *us-east-1* pela região em que você deseja remover essa conta.
2. Para remover uma ou mais contas de GuardDuty membros, execute DisassociateMemberspara remover a conta de membro associada à conta de administrador.

   Como alternativa, você pode usar AWS CLI para executar o seguinte comando:

   ```
   aws guardduty disassociate-members --detector-id 12abc34d567e8fa901bc2d34EXAMPLE
    --account-ids 111122223333 --region us-east-1
   ```

   Substitua *us-east-1* pela região em que você deseja remover essa conta. Caso tenha uma lista de IDs da conta que deseja remover, separe-os com um caractere de espaço.

Excluindo contas de membros da organização GuardDuty

Como conta de GuardDuty administrador delegado, depois de desassociar uma conta de membro e não querer mais manter essa conta de membro na GuardDuty organização, você pode excluir essa conta de membro da sua GuardDuty organização. Essa conta-membro não aparecerá mais no inventário da sua conta. No entanto, se não GuardDuty foi suspenso nessa conta de membro, a configuração GuardDuty e os planos de proteção dedicados permanecem os mesmos. Essa conta agora se tornará uma conta independente e poderá GuardDuty se desativar sozinha.

Essa etapa não excluirá a conta do membro da sua AWS organização.

Escolha um método preferido para excluir uma conta de membro da sua GuardDuty organização.

Console

1. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.

   Para entrar, use as credenciais da conta de GuardDuty administrador delegado.
2. No painel de navegação, selecione Contas.
3. Na tabela Contas, remova uma conta que tenha Tipo como Via Organizações e Status como Removido (desassociado).

   Selecione uma ou mais contas com o mesmo Tipo e Status.
4. No menu suspenso Ações, selecione Excluir conta.
5. Selecione Excluir contas para confirmar sua seleção. O membro da conta selecionado não aparecerá mais em sua tabela de Contas.

   Repita as etapas anteriores em cada região adicional onde deseja excluir essa conta-membro.

API/CLI

1. Para recuperar o ID da conta-membro que deseja excluir, use a API ListMembers. Inclua o parâmetro `OnlyAssociated` na sua solicitação. Se você definir o valor desse parâmetro como`false`, GuardDuty retornará uma `members` matriz que fornece detalhes somente sobre as contas que atualmente são GuardDuty membros desassociados.

   Como alternativa, você pode usar AWS Command Line Interface (AWS CLI) para executar o seguinte comando:

   ```
   aws guardduty list-members --detector-id 12abc34d567e8fa901bc2d34EXAMPLE --only-associated="false" --region us-east-1
   ```

   *12abc34d567e8fa901bc2d34EXAMPLE*Substitua pelo ID do detector da conta de GuardDuty administrador *us-east-1* delegado e pela região em que você deseja remover essa conta.
2. Para excluir uma ou mais contas de GuardDuty membros, execute DeleteMemberspara excluir a conta de membro da GuardDuty organização.

Como alternativa, você pode usar AWS CLI para executar o seguinte comando:

```
aws guardduty delete-members --detector-id 12abc34d567e8fa901bc2d34EXAMPLE --
account-ids 111122223333 --region us-east-1
```

*12abc34d567e8fa901bc2d34EXAMPLE*Substitua pelo ID do detector da conta de GuardDuty administrador delegado e *us-east-1* pela região em que você deseja remover essa conta. Caso tenha uma lista de IDs da conta que deseja remover, separe-os com um caractere de espaço.

Alterando a conta do GuardDuty administrador delegado

Você pode remover a conta de GuardDuty administrador delegado da sua organização em cada região e, em seguida, delegar um novo administrador em cada região. Para manter a postura de segurança das contas dos membros da sua organização em uma região, você deve ter uma conta de GuardDuty administrador delegada nessa região.

> **Observação**
>
> Antes de remover uma conta de GuardDuty administrador delegado, você deve desassociar todas as contas de membros associadas à conta de GuardDuty administrador delegado e, em seguida, excluí-las da organização. GuardDuty Para obter mais informações sobre essas etapas, consulte os documentos a seguir:
>
> - Como desassociar (remover) a conta-membro da conta de administrador
> - Excluindo contas de membros da organização GuardDuty

Removendo a conta de GuardDuty administrador delegado existente

Etapa 1 - Para remover a conta de GuardDuty administrador delegado existente em cada região

1. Como conta de GuardDuty administrador delegado existente, liste todas as contas de membros vinculadas à sua conta de administrador. Executar ListMembers com `OnlyAssociated=false`.
2. Se a preferência de ativação automática GuardDuty ou qualquer um dos planos de proteção opcionais estiver definida como`ALL`, execute UpdateOrganizationConfigurationpara atualizar a

configuração da organização para `NEW` ou`NONE`. Essa ação evitará um erro ao desassociar todas as contas-membro na próxima etapa.

3. Execute DisassociateMembers para desassociar todas as contas-membro associadas à conta do administrador.
4. Execute DeleteMembers para excluir as associações entre a conta do administrador e as contas-membro.
5. Como conta de gerenciamento da organização, execute DisableOrganizationAdminAccountpara remover a conta de GuardDuty administrador delegado existente.
6. Repita essas etapas em cada um Região da AWS em que você tenha essa conta de GuardDuty administrador delegado.

Etapa 2 - Para cancelar o registro da conta de GuardDuty administrador delegado existente no AWS Organizations (ação One-time global)

- Execute DeregisterDelegatedAdministratorna Referência da AWS Organizations API para cancelar o registro da conta de GuardDuty administrador delegado existente em. AWS Organizations

  Como alternativa, você pode executar o seguinte AWS CLI comando:

  ```
  aws organizations deregister-delegated-administrator --account-id 111122223333 --
  service-principal guardduty.amazonaws.com
  ```

  Certifique-se de *111122223333* substituir pela conta de GuardDuty administrador delegado existente.

  Depois de cancelar o registro da antiga conta de GuardDuty administrador delegado, você pode adicioná-la como uma conta de membro à nova conta de administrador delegado GuardDuty .

Designação de uma nova conta de GuardDuty administrador delegado em cada região

1. Designe uma nova conta de GuardDuty administrador delegado em cada região usando seu método de acesso preferido: GuardDuty console, API ou. AWS CLI Para obter mais informações, consulte Designação de uma conta de administrador delegado GuardDuty.
2. Execute DescribeOrganizationConfigurationpara ver a configuração atual de ativação automática da sua organização.

> **Important**
>
> Antes de adicionar qualquer membro à nova conta de GuardDuty administrador delegado, você deve verificar a configuração de ativação automática da sua organização. Essa configuração é específica para a nova conta de GuardDuty administrador delegado e para a região selecionada, e não está relacionada a. AWS Organizations Quando você adiciona uma conta de membro da organização (nova ou existente) à nova conta de GuardDuty administrador delegado, a configuração de ativação automática da nova conta de GuardDuty administrador delegado será aplicada no momento da ativação GuardDuty ou de qualquer um de seus planos de proteção opcionais.

Altere a configuração da organização para a nova conta de GuardDuty administrador delegado usando seu método de acesso preferido: GuardDuty console, API ou AWS CLI. Para obter mais informações, consulte Como configurar as preferências de habilitação automática da organização.

Gerenciando contas usando as políticas da organização

Uma política GuardDuty organizacional permite que você habilite e gerencie centralmente a Amazon GuardDuty em todas as contas da sua organização. Você usa uma política AWS Organizations declarativa para especificar quais entidades organizacionais (raiz da organização, unidades organizacionais (OUs) ou contas individuais) têm o detector GuardDuty básico e seus planos de proteção ativados e gerenciados automaticamente por meio da conta de administrador delegado GuardDuty . As contas que ingressam na organização ou se mudam para uma OU que tem uma política anexada herdam a política GuardDuty e têm seus planos de proteção configurados de acordo com o que a política efetiva define para elas.

GuardDuty as políticas da organização são um mecanismo diferente das configurações de ativação automática descritas emGerenciando GuardDuty contas com AWS Organizations. Para o conceito de política, estrutura, herança, validação e exemplos de políticas, consulte GuardDutypolíticas no Guia do AWS Organizations usuário.

Conteúdos

- Pré-requisitos

- Como as políticas da organização funcionam
- Criação de uma política no console
- Analisar o impacto de uma política antes de aplicá-la
- Considerações e limitações

Pré-requisitos

Antes de usar as políticas GuardDuty da organização, preencha os seguintes pré-requisitos:

- Habilite o acesso confiável para o GuardDuty serviço em AWS Organizations.
- Atribua uma conta de GuardDuty administrador delegado.
- Anexe a política de delegação que concede permissão ao administrador delegado para gerenciar GuardDuty políticas.
- Habilite o tipo de política `GUARDDUTY_POLICY` na raiz da organização. Isso acontece automaticamente quando o administrador delegado cria a primeira política no GuardDuty console.

> **Warning**
>
> A ativação do tipo de `GUARDDUTY_POLICY` política impede que as configurações regionais de GuardDuty ativação automática sejam aplicadas, mesmo antes de você anexar uma política. Como o console habilita esse tipo de política automaticamente quando o administrador delegado cria a primeira política, você pode parar de confiar na ativação automática sem querer. Revise sua configuração de ativação automática existente antes de criar sua primeira política.

Para ver as etapas detalhadas, consulte GuardDutyas políticas no Guia AWS Organizations do usuário.

Como as políticas da organização funcionam

A política GuardDuty da organização determina quais GuardDuty recursos estão habilitados, em quais regiões e para quais contas. As seções a seguir descrevem como uma política se aplica em todas as regiões, como as políticas são herdadas por sua organização, como uma política ativa muda a maneira como você gerencia GuardDuty contas e formas comuns de usar uma política.

Conteúdo

- Configuração regional
- Herança e precedência de políticas
- Como uma política afeta o gerenciamento de GuardDuty contas
- Exemplo de casos de uso

Configuração regional

A política GuardDuty da organização define a capacitação por região. A configuração padrão se aplica a todas as regiões em que GuardDuty está disponível. Você pode adicionar uma substituição regional para dar a uma região específica uma configuração diferente. A configuração padrão é opcional. Se você omitir isso, somente as regiões especificadas serão gerenciadas e todas as outras regiões ficarão sem gerenciamento.

Quando uma política é ativada de GuardDuty forma ampla, como uma configuração padrão que cobre todas as regiões, GuardDuty processa eventos de serviços AWS CloudTrail globais em todas as regiões em que ela está ativada, incluindo regiões nas quais você não tem recursos ou cargas de trabalho. Para obter mais informações, consulte Como GuardDuty manuseia AWS CloudTrail eventos globais.

Uma política é gerenciada GuardDuty e um plano de proteção somente nas regiões em que elas estão disponíveis. Se sua política habilitar GuardDuty ou um plano de proteção em uma região onde ele não estiver disponível, a política o ignorará nessa região sem cometer erros. Antes de configurar uma política, revise onde GuardDuty e cada plano de proteção está disponível. Para obter mais informações, consulte Region-specific disponibilidade de recursos.

Uma substituição regional substitui totalmente a configuração padrão dessa região. Ele não se mescla com o padrão, portanto, você deve especificar cada plano de proteção que deseja gerenciar nessa região. Qualquer plano de proteção que você deixe de fora de uma substituição não é gerenciado nessa região, mesmo que a configuração padrão o gerencie. Por esse motivo, os planos de proteção gerenciados por uma política podem diferir de uma região para outra.

Para ver a estrutura política completa e como as regiões são resolvidas, consulte GuardDuty as políticas no Guia AWS Organizations do Usuário.

Herança e precedência de políticas

GuardDuty as políticas da organização seguem o AWS Organizations modelo de herança. Uma política anexada na raiz da organização se aplica a todas as contas da organização. As contas também herdam qualquer política vinculada a uma OU principal. Quando mais de uma política se aplica a uma conta, ela é AWS Organizations mesclada em uma única política efetiva, e uma política anexada mais próxima à conta tem precedência sobre outra anexada no topo da hierarquia.

Depois de habilitar o tipo de `GUARDDUTY_POLICY` política, a política tem precedência sobre as configurações regionais de GuardDuty ativação automática. As configurações de ativação automática não se aplicam mais, independentemente de uma política estar anexada ou não.

Para obter as regras completas de herança e como a política efetiva é resolvida, consulte Entendendo a herança da política de gerenciamento no Guia do usuário. AWS Organizations

Como uma política afeta o gerenciamento de GuardDuty contas

Quando uma política GuardDuty da organização está ativa, as seguintes alterações se aplicam à forma como você gerencia GuardDuty as contas:

- Depois que o tipo de `GUARDDUTY_POLICY` política é ativado, as configurações regionais de GuardDuty ativação automática não se aplicam mais, independentemente de uma política estar ou não anexada.
- Quando uma política gerencia um plano de proteção, esse plano de proteção não pode mais ser alterado por meio do GuardDuty console ou da API das contas cobertas. Na página Contas, ela aparece como Política gerenciada. Para alterar um plano de proteção gerenciado, atualize a política. Os planos de proteção que a política não gerencia permanecem editáveis por meio do console e da API.
- Somente a conta de administrador delegado pode criar e gerenciar GuardDuty políticas. A página Políticas da organização no GuardDuty console está disponível somente para o administrador delegado.

> **Note**
>
> Anexar uma GuardDuty política pode inscrever novas contas como GuardDuty membros e ativar planos de proteção em toda a organização. A habilitação GuardDuty e seus planos

de proteção incorrem em cobranças. Para obter mais informações, consulte Preços em GuardDuty.

Exemplo de casos de uso

Os exemplos a seguir mostram formas comuns de usar uma política GuardDuty da organização. Para a política JSON que implementa cada padrão, consulte GuardDuty as políticas no Guia do AWS Organizations usuário.

- Habilite uma linha de base de proteção em toda a organização. Anexe uma política na raiz da organização com uma configuração padrão que habilite o detector básico e os planos de proteção necessários. Todas as contas, incluindo contas que se cadastram posteriormente, ativam esses recursos automaticamente.
- Varie a proteção por unidade organizacional. Use uma política ampla como base para sua linha de base e anexe políticas mais específicas a OUs individuais para ajustar os planos de proteção para contas com diferentes requisitos de conformidade ou carga de trabalho.
- Mantenha a cobertura à medida que sua organização cresce. Como as contas que ingressam na organização ou se mudam para uma OU coberta herdam a política efetiva, uma política mantém as contas recém-criadas alinhadas com sua linha de base de proteção sem a ativação manual.

Criação de uma política no console

Você cria e gerencia GuardDuty políticas a partir da conta de administrador delegado, na página Políticas da organização no GuardDuty console. Criar sua primeira política também ativa automaticamente o tipo de `GUARDDUTY_POLICY` política para sua organização.

Para criar uma GuardDuty política

1. Entre no GuardDuty console com a conta de administrador delegado.
2. No painel de navegação, escolha Políticas da organização e, em seguida, escolha Criar política.
3. Em Etapa 1: Detalhes da política, insira um nome de política e uma descrição opcional e escolha Avançar.
4. Para a Etapa 2: Contas, escolha onde a política está anexada na hierarquia da sua organização e, em seguida, escolha Avançar:

   - Todas as unidades organizacionais e contas anexam a política em toda a organização.

- Unidades organizacionais e contas específicas o anexam às entidades que você seleciona.
- Nenhuma unidade organizacional ou conta cria a política sem anexá-la.

5. Para a Etapa 3: Detalhes da configuração, em Seleção de capacidade, selecione os planos de proteção que essa política gerencia. Use Ativar tudo ou Desativar tudo para um ponto de partida rápido e, em seguida, ajuste os planos de proteção individuais. Os planos de proteção que você não seleciona não são afetados por essa política. A detecção básica de ameaças deve ser ativada se você ativar qualquer outro plano de proteção. Escolha Próximo.
6. (Opcional) Para a Etapa 4: substituições regionais, escolha Adicionar substituição regional, selecione uma ou mais regiões e defina a configuração para essas regiões. Uma substituição regional substitui totalmente a configuração padrão da Região, portanto, especifique cada plano de proteção que você deseja gerenciar lá. Escolha Próximo.
7. Para a Etapa 5: revisar e criar, revise os detalhes da política, as contas, a configuração padrão e quaisquer substituições regionais. Para ver o JSON da política gerada, expanda Documento de política. Selecione Criar política.

Você pode revisar ou editar o JSON gerado em qualquer etapa expandindo o documento de política. Para ver a estrutura da política, as regras de herança e os exemplos de políticas, consulte as GuardDutypolíticas no Guia do AWS Organizations usuário.

Analisar o impacto de uma política antes de aplicá-la

Antes de salvar uma alteração de política que desabilita um plano de proteção, analise quais contas e regiões têm esse plano de proteção ativado no momento, para que você entenda o que a alteração desativará. Como uma GuardDuty política se aplica por região, verifique o estado atual de habilitação por conta e por região.

> **Warning**
>
> Uma política que desativa GuardDuty ou um plano de proteção a desativa em todas as contas cobertas em que ela está atualmente habilitada e impede que essas contas a reativem por meio do console ou da API. Você pode desativar involuntariamente a proteção da qual as contas dependem. Antes de criar ou atualizar uma política, identifique as contas e regiões afetadas pela alteração, conforme descrito nesta seção, e confirme se o impacto é pretendido.

Como administrador delegado, você pode revisar a GuardDuty capacitação atual em sua organização usando a página GuardDuty Contas do console (alterne as regiões para revisar a cobertura em cada região) ou programaticamente com as etapas a seguir. Execute as etapas da API em cada região que você deseja revisar.

Identificar as contas e regiões que uma política afeta

1. Enumere as contas em sua organização. Use a operação de AWS Organizations `ListAccounts` API para listar todas as contas da organização, incluindo contas que ainda não são GuardDuty membros.
2. Enumere suas contas de membros. GuardDuty Use a operação de GuardDuty `ListMembers` API para listar as contas que já são contas de GuardDuty membros.
3. Revise os planos de proteção habilitados para cada conta de membro. Use a operação da GuardDuty `GetMemberDetectors` API para ver quais recursos estão habilitados para o detector de cada conta de membro.
4. Compare a capacitação atual com os planos de proteção que sua alteração de política desativará para identificar as contas e regiões que a mudança afeta.

Uma conta que pertence à sua organização, mas ainda não é GuardDuty membro`ListMembers`, não aparece e você não pode ver o status do detector até adicioná-la como membro. Quando uma GuardDuty política se aplica a uma conta que ainda não é membro, a conta é adicionada automaticamente como membro.

Depois de criar e anexar uma política, confirme a política final que se aplica a uma conta específica. A política efetiva é a agregação de todas as políticas que a conta herda de suas entidades controladoras, combinada com qualquer política vinculada diretamente à conta. Para visualizá-la, use a operação de AWS Organizations `DescribeEffectivePolicy` API, ou seus equivalentes de AWS CLI ou AWS SDK, com o tipo de política. GuardDuty Qualquer conta com permissão para chamar essa operação pode usá-la, incluindo a conta de administrador delegado. Para obter mais informações, consulte Visualização de políticas declarativas efetivas no Guia do AWS Organizations usuário.

Considerações e limitações

Lembre-se do seguinte ao planejar e gerenciar as políticas GuardDuty da organização:

- Uma política se aplica somente às contas em AWS Organizations. Uma política da organização pode ser gerenciada GuardDuty somente em contas que pertencem à sua organização por meio

de AWS Organizations. Ele não pode gerenciar contas que não fazem parte da sua organização, como contas associadas somente pelo método de convite antigo. Gerencie GuardDuty essas contas separadamente, a partir da conta de GuardDuty administrador delegado ou em cada conta. Para obter mais informações sobre os dois métodos de associação, consulte Gerenciando várias contas na Amazon GuardDuty.

- Uma política pode ser GuardDuty ativada na conta de gerenciamento somente se a função vinculada ao serviço já existir lá. Uma política não pode ser GuardDuty ativada na conta de gerenciamento da organização, a menos que a função GuardDuty vinculada ao serviço já exista nessa conta. Se a função estiver ausente, GuardDuty ela não será ativada na conta de gerenciamento, mesmo quando a política a declarar ativada. Crie a função na conta de gerenciamento, por exemplo, GuardDuty habilitando-a, antes de confiar em uma política para gerenciá-la.
- O administrador delegado é atribuído por região, e habilitar contas é diferente de visualizá-las. A conta de gerenciamento designa o administrador GuardDuty delegado em cada região. Um administrador delegado atribuído em uma região pode criar uma política que habilite contas GuardDuty de membros, inclusive em regiões onde não é o administrador delegado. No entanto, o administrador delegado não pode ver o status ou as descobertas dessas contas membros em uma região, a menos que a conta de gerenciamento também o tenha designado como administrador delegado nessa região. Para gerenciar e monitorar contas de membros em uma região, a conta de gerenciamento deve designar o administrador delegado nessa região. Como a designação é por região, a conta de gerenciamento pode designar contas diferentes como administradoras delegadas em diferentes regiões, e cada administrador delegado gerencia e monitora contas de membros somente nas regiões em que é designada.
- O administrador delegado precisa da política de AWS Organizations delegação para gerenciar as políticas. A designação de um administrador delegado permite que ele visualize as contas dos membros, mas não pode criar, atualizar ou anexar políticas GuardDuty da organização, a menos que a política de AWS Organizations delegação também conceda permissão para gerenciar o tipo de `GUARDDUTY_POLICY` política. Se essas operações forem negadas, verifique se a política de delegação concede permissão ao administrador delegado para gerenciar o tipo de política.
- Um plano de proteção gerenciado é somente para leitura no console e na API. Quando uma política gerencia um plano de proteção, as contas cobertas não podem alterá-lo por meio do GuardDuty console ou da API. Para alterar um plano de proteção gerenciado, atualize a política. Os planos de proteção que a política não gerencia permanecem editáveis por meio do console e da API.

- Uma política gerencia somente a capacitação, não as personalizações de detecção. Uma política GuardDuty organizacional ativa e desativa GuardDuty seus planos de proteção. Ele não gerencia personalizações de detecção, como listas de entidades, listas de endereços IP ou regras de supressão. Configure-os separadamente por meio do GuardDuty console ou da API após GuardDuty ativá-los. Para obter mais informações, consulte Customizing threat detection with entity lists and IP address lists e Regras de supressão em GuardDuty.
- Uma região não gerenciada é deixada inalterada, não desativada. Uma região que uma política não inclui na configuração padrão nem nomeia em uma substituição regional não é gerenciada. A política não é ativada nem desativada GuardDuty lá, e as configurações existentes nessa região são deixadas como estão.
- GuardDuty processa eventos globais em todas as regiões habilitadas. GuardDuty replica eventos de serviços AWS CloudTrail globais, de serviços como IAM, Amazon S3 e CloudFront Amazon AWS STS, e os processa em todas as regiões em que está habilitado, incluindo regiões nas quais você não tem recursos ou cargas de trabalho. GuardDuty Isso melhora a detecção de ameaças, mas significa que, quando uma política é GuardDuty amplamente ativada, como uma configuração padrão que cobre todas as regiões, GuardDuty processa esses eventos globais em todas essas regiões, o que pode gerar custos adicionais GuardDuty . Para obter mais informações, consulte Como GuardDuty manuseia AWS CloudTrail eventos globais e Preços em GuardDuty.
- A desativação de um plano de proteção o desativa onde ele está habilitado no momento. Uma política que desativa GuardDuty ou um plano de proteção a desativa em todas as contas cobertas em que ela está ativada e impede que essas contas a ativem novamente por meio do console ou da API. Antes de criar ou atualizar uma política, identifique as contas e regiões que a alteração afeta, conforme descrito emAnalisar o impacto de uma política antes de aplicá-la.
- As alterações de política se aplicam de forma assíncrona. Uma mudança de política se propaga por toda a organização e é reconciliada ao longo do tempo, em vez de entrar em vigor instantaneamente. Reserve um tempo para que uma alteração seja aplicada antes de concluir que ela não entrou em vigor.
- A desanexação de uma política não desativa GuardDuty. Quando você separa uma política GuardDuty organizacional de uma entidade, outras políticas que a entidade herda das entidades principais ainda podem ser aplicadas e continuar governando o alvo. Se nenhuma política efetiva permanecer após a separação, GuardDuty seus planos de proteção permanecerem em seu estado atual e não forem desativados. Em ambos os casos, alterações futuras em sua organização, como a entrada de novas contas ou a migração de contas existentes para uma OU, não serão mais ativadas GuardDuty automaticamente, a menos que uma política herdada ainda as cubra.

Qualquer habilitação adicional deve ser feita manualmente, anexando novamente uma política ou por meio de uma política herdada.

- A desativação do tipo de política interrompe todo o gerenciamento de políticas e restaura a ativação automática. Desabilitar GuardDuty em uma política, desanexar uma política e desabilitar o tipo de `GUARDDUTY_POLICY` política são três ações diferentes com efeitos diferentes. Quando você desativa o tipo de `GUARDDUTY_POLICY` política na raiz da GuardDuty organização, as políticas da organização não governam mais nenhuma conta e GuardDuty permanecem habilitadas nas contas cobertas anteriormente. A desativação do tipo de política também restaura as configurações regionais de GuardDuty ativação automática que a ativação do tipo de política havia suprimido, portanto, a ativação automática é retomada de acordo com essas configurações.

Gerenciando GuardDuty contas por convite

Para gerenciar contas externas à organização, é possível usar o método de convite legado. Ao usar esse método, sua conta é designada como uma conta de administrador quando outra conta aceita seu convite para se tornar uma conta de membro.

> **Note**
>
> GuardDuty recomenda usar, AWS Organizations em vez de GuardDuty convites, para gerenciar suas contas de membros. Para obter mais informações, consulte Como gerenciar contas com o AWS Organizations.

Caso sua conta não seja uma conta de administrador, você pode aceitar um convite de outra conta. Ao aceitar, sua conta se tornará uma conta de membro. Uma AWS conta não pode ser uma conta de GuardDuty administrador e uma conta de membro ao mesmo tempo.

Ao aceitar um convite de uma conta, você não pode aceitar um convite de outra conta. Para aceitar um convite de outra conta, primeiro é preciso desassociar sua conta da conta de administrador vigente. Outra alternativa é que a conta de administrador também pode desassociar e remover sua conta da organização.

As contas associadas por convite têm uma relação geral de administrador entre contas e membros semelhante à das contas associadas por AWS Organizations, conforme descrito em. Entendendo a relação entre a conta GuardDuty do administrador e as contas dos membros No entanto, os usuários da conta de administrador de convites não podem habilitar GuardDuty em nome de contas

de membros associados ou visualizar outras contas de não membros em sua AWS Organizations organização.

> **Important**
>
> Cross-regional a transferência de dados pode ocorrer ao GuardDuty criar contas de membros usando esse método. Para verificar os endereços de e-mail das contas dos membros, GuardDuty usa um serviço de verificação de e-mail que opera somente na região Leste dos EUA (Norte da Virgínia).

Tópicos

- Adição de contas por convite
- Consolidação de contas de GuardDuty administrador em uma única organização

Adição de contas por convite

Como uma conta de administrador que já foi GuardDuty ativada, você pode adicionar membros para começar a usar GuardDuty. Depois de adicionar os membros, você pode convidá-los a participar GuardDuty e eles podem escolher responder ao seu convite.

> **Note**
>
> GuardDuty recomenda usar, AWS Organizations em vez de GuardDuty convites, para gerenciar suas contas de membros. Para obter mais informações, consulte Como gerenciar contas com o AWS Organizations.

Escolha um método de acesso preferido para adicionar contas de GuardDuty membros como conta de GuardDuty administrador.

Console

Etapa 1 – Adicionar uma conta

1. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.
2. No painel de navegação, selecione Contas.
3. Selecione Adicionar contas por convite no painel superior.

4. Na página Adicionar contas-membro, em Inserir detalhes da conta, digite o ID e o endereço de e-mail da Conta da AWS associados à conta que você deseja adicionar.
5. Para adicionar outra linha para inserir os detalhes da conta, um por vez, escolha Adicionar outra conta. Você também pode escolher Carregar arquivo.csv com detalhes da conta para adicionar contas em massa.

   > **Important**
   >
   > A primeira linha do arquivo .csv deve conter o cabeçalho, como ilustrado no exemplo a seguir: `Account ID,Email`. Cada linha subsequente deve conter uma única Conta da AWS ID válida e o endereço de e-mail associado. O formato de uma linha é válido se ela contiver somente um ID de Conta da AWS e o endereço de e-mail associado separados por uma vírgula.
   >
   > ```
   > Account ID,Email
   > 555555555555,user@example.com
   > ```

6. Depois de adicionar todos os detalhes das contas, escolha Próximo. Você pode ver as contas recém-adicionadas na tabela Contas. O status dessas contas será Convite não enviado. Para obter informações sobre como enviar um convite para uma ou mais contas adicionadas, consulte Step 2 - Invite an account.

Etapa 2: convidar uma conta

1. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.
2. No painel de navegação, selecione Contas.
3. Selecione uma ou mais contas que você deseja convidar para a Amazon GuardDuty.
4. Selecione o menu suspenso Ações e, em seguida, selecione Convidar.
5. Na caixa de GuardDuty diálogo Convite para, insira uma mensagem de convite (opcional).

   Se a conta convidada não tiver acesso ao e-mail, marque a caixa de seleção Também enviar uma notificação por e-mail para o usuário raiz na conta do convidado Conta da AWS e gerar um alerta na conta do convidado. AWS Health Dashboard
6. Selecione Enviar convite. Se os convidados tiverem acesso ao endereço de e-mail especificado, eles poderão ver o convite abrindo o GuardDuty console em. https://console.aws.amazon.com/guardduty/

7. Quando um convidado aceita o convite, o valor na coluna Status muda para Convidado. Para obter informações sobre como gerenciar um convite, consulte Step 3 - Accept an invitation.

Etapa 3: aceitar um convite

1. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.

   > **Important**
   >
   > Você deve habilitar GuardDuty antes de poder ver ou aceitar um convite de associação.

2. Faça o seguinte somente se você GuardDuty ainda não tiver ativado; caso contrário, você pode pular essa etapa e continuar com a próxima etapa.

   Se você ainda não habilitou GuardDuty, escolha Get Started na GuardDuty página da Amazon.

   Na página Bem-vindo GuardDuty, escolha Habilitar GuardDuty.

3. Depois de ativar GuardDuty sua conta, use as etapas a seguir para aceitar o convite de associação:

   a. No painel de navegação, selecione Configurações.

   b. Selecione Contas.

   c. Em Contas, certifique-se de verificar o proprietário da conta da qual você aceita o convite. Habilite a opção Aceitar para aceitar o convite de membro.

4. Depois de aceitar o convite, sua conta se torna uma conta de GuardDuty membro. A conta cujo proprietário enviou o convite se torna a conta GuardDuty do administrador. A conta do administrador saberá que você aceitou o convite. A tabela de contas em sua GuardDuty conta será atualizada. O valor na coluna Status correspondente ao ID da sua conta de membro será alterado para Habilitado. O proprietário da conta de administrador agora pode visualizar GuardDuty e gerenciar as configurações do plano de proteção em nome da sua conta. A conta do administrador também pode visualizar e gerenciar GuardDuty as descobertas geradas para sua conta de membro.

API/CLI

Você pode designar uma conta de GuardDuty administrador e criar ou adicionar contas de GuardDuty membros por convite por meio das operações da API. Execute as seguintes operações de GuardDuty API para designar contas de administrador e contas de membros em GuardDuty.

Conclua o procedimento a seguir usando as credenciais da Conta da AWS que você deseja designar como conta de GuardDuty administrador.

Criação ou adição de contas-membro

1. Execute a operação da CreateMembersAPI usando as credenciais da AWS conta que foi GuardDuty ativada. Essa é a conta que você deseja que seja a GuardDuty conta de administrador.

   Você deve especificar o ID do detector da AWS conta atual e o ID da conta e o endereço de e-mail das contas das quais você deseja que se tornem GuardDuty membros. É possível criar um ou mais membros com essa operação de API.

   Você também pode usar as ferramentas de linha de AWS comando para designar uma conta de administrador executando o seguinte comando da CLI. Use seu próprio ID de detector válido, ID da conta e e-mail.

   Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no https://console.aws.amazon.com/guardduty/console ou execute a ListDetectorsAPI.

   ```
   aws guardduty create-members --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
   account-details AccountId=111122223333,Email=guardduty-member@organization.com
   ```

2. Execute InviteMembersusando as credenciais da AWS conta que foi GuardDuty ativada. Essa é a conta que você deseja que seja a GuardDuty conta de administrador.

   Você deve especificar o ID do detector da AWS conta atual e os IDs das contas das quais você deseja que se tornem GuardDuty membros. Você pode convidar um ou mais membros com essa operação de API.

> **Note**
>
> Você também pode especificar uma mensagem de convite opcional usando o parâmetro de solicitação `message`.

Você também pode usar AWS Command Line Interface para designar contas de membros executando o comando a seguir. Use seu próprio ID de detector e IDs válidos das contas que deseja convidar.

Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no https://console.aws.amazon.com/guardduty/console ou execute a ListDetectorsAPI.

```
aws guardduty invite-members --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
account-ids 111122223333
```

Como aceitar convites

Conclua o procedimento a seguir usando as credenciais de cada AWS conta que você deseja designar como conta de GuardDuty membro.

1. Execute a operação da CreateDetectorAPI para cada AWS conta que foi convidada para se tornar uma conta GuardDuty membro e que você deseja aceitar um convite.

   Você deve especificar se o recurso do detector deve ser ativado usando o GuardDuty serviço. Um detector deve ser criado e ativado para que ele GuardDuty se torne operacional. Você deve primeiro habilitar GuardDuty antes de aceitar um convite.

   Você também pode fazer isso usando as ferramentas de linha de AWS comando usando o seguinte comando da CLI.

   ```
   aws guardduty create-detector --enable
   ```

2. Execute a operação da AcceptAdministratorInvitationAPI para cada AWS conta em que você deseja aceitar o convite de associação, usando as credenciais dessa conta.

Você deve especificar o ID do detector dessa AWS conta para a conta do membro, o ID da conta do administrador que enviou o convite e o ID do convite que você está aceitando. É possível encontrar o ID da conta de administrador no e-mail de convite ou usando a operação de API ListInvitations.

Você também pode aceitar um convite usando as ferramentas de linha de AWS comando executando o seguinte comando da CLI. Use um ID de detector válido, um ID de conta de administrador e um ID de convite.

Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no https://console.aws.amazon.com/guardduty/console ou execute a ListDetectorsAPI.

```
aws guardduty accept-invitation --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --administrator-id 444455556666 --invitation-
id 84b097800250d17d1872b34c4daadcf5
```

Consolidação de contas de GuardDuty administrador em uma única organização

GuardDuty recomenda usar a associação AWS Organizations para gerenciar contas de membros em uma conta de GuardDuty administrador delegado. Você pode usar o processo de exemplo descrito abaixo para consolidar a conta de administrador e o membro associado por convite em uma organização em uma única conta de administrador GuardDuty delegado GuardDuty .

> **Note**
>
> GuardDuty recomenda usar, AWS Organizations em vez de GuardDuty convites, para gerenciar suas contas de membros. Para obter mais informações, consulte Como gerenciar contas com o AWS Organizations.

Contas que já estão sendo gerenciadas por uma conta de GuardDuty administrador delegado ou contas de membros ativas associadas à conta de GuardDuty administrador delegado não podem ser adicionadas a uma conta de administrador delegado GuardDuty diferente. Cada organização pode ter somente uma conta de GuardDuty administrador delegado por região, e cada conta de membro pode ter somente uma conta de GuardDuty administrador delegado.

Escolha um método de acesso preferencial para consolidar contas de GuardDuty administrador em uma única conta de GuardDuty administrador delegado.

Console

1. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.

   Para fazer login, use as credenciais da conta de gerenciamento da organização.
2. Todas as contas que você deseja gerenciar GuardDuty devem fazer parte da sua organização. Para obter informações sobre como adicionar uma conta à sua organização, consulte Convidar um Conta da AWS para participar da sua organização.
3. Certifique-se de que todas as contas dos membros estejam associadas à conta que você deseja designar como a única conta de GuardDuty administrador delegado. Desassocie qualquer conta de membro que ainda esteja associada às contas de administrador preexistentes.

   As etapas a seguir ajudarão você a desassociar contas-membro da conta de administrador preexistente:

   a. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.
   b. Para fazer login, use as credenciais da conta de administrador preexistente.
   c. No painel de navegação, selecione Contas.
   d. Na página Contas, selecione uma ou mais contas que você deseja desassociar da conta de administrador.
   e. Selecione Ações e, em seguida, selecione Desassociar conta.
   f. Selecione Confirmar para finalizar a etapa.
4. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.

   Para fazer login, use as credenciais da conta de gerenciamento.
5. No painel de navegação, selecione Configurações. Na página Configurações, designe a conta de GuardDuty administrador delegado para a organização.
6. Faça login na conta de GuardDuty administrador delegado designada.
7. Adicionar membros da organização. Para obter mais informações, consulte Gerenciando GuardDuty contas com AWS Organizations.

API/CLI

1. Todas as contas que você deseja gerenciar GuardDuty devem fazer parte da sua organização. Para obter informações sobre como adicionar uma conta à sua organização, consulte Convidar um Conta da AWS para participar da sua organização.
2. Certifique-se de que todas as contas dos membros estejam associadas à conta que você deseja designar como a única conta de GuardDuty administrador delegado.

   a. Execute DisassociateMemberspara desassociar qualquer conta de membro que ainda esteja associada às contas de administrador preexistentes.

   b. Como alternativa, você pode usar AWS Command Line Interface para executar o comando a seguir e *777777777777* substituí-lo pelo ID do detector da conta de administrador preexistente da qual você deseja desassociar a conta do membro. *666666666666*Substitua pelo Conta da AWS ID da conta de membro que você deseja desassociar.

   ```
   aws guardduty disassociate-members --detector-id 777777777777 --account-
   ids 666666666666
   ```

3. Execute EnableOrganizationAdminAccountpara delegar uma Conta da AWS como conta de GuardDuty administrador delegado.

   Como alternativa, você pode usar AWS Command Line Interface para executar o seguinte comando para delegar uma conta de GuardDuty administrador delegado:

   ```
   aws guardduty enable-organization-admin-account --admin-account-id 777777777777
   ```

4. Adicionar membros da organização. Para obter mais informações, consulte Create or add member member accounts using API.

> **Important**
>
> Para maximizar a eficácia de GuardDuty um serviço regional, recomendamos que você designe sua conta de GuardDuty administrador delegado e adicione todas as suas contas de membros em cada região.

GuardDuty considerações para exportar detalhes da conta do membro no formato CSV

Como conta de GuardDuty administrador, você pode exportar os detalhes da conta do membro em formato CSV. Esses detalhes incluem o ID da conta do membro, nome, tipo (adicionado por AWS Organizations ou por meio de convite) e status de configuração GuardDuty e planos de proteção dedicados.

A opção Exportar CSV é exibida na página GuardDuty Contas com base em como você gerencia as contas de vários membros. Ao usar a opção Exportar CSV, você pode identificar quais contas de membros têm um plano de proteção específico ativado.

A lista a seguir fornece os critérios para saber se o CSV de exportação estará ou não disponível na sua página GuardDuty Contas:

- Você usa apenas AWS Organizations para gerenciar várias contas de membros e o número total de contas de membros em sua GuardDuty organização é de até 5.000.
- Você usa o método de convites AWS Organizations e o número total de contas de membros em sua GuardDuty organização é de até 5.000.

  Nesse cenário, o CSV exportado incluirá se uma conta de membro foi adicionada por meio de AWS Organizations ou usando o método baseado em convite.
- Quando você usa somente o método baseado em convite para gerenciar várias contas de membros, não há a opção de Exportar CSV.

GuardDuty tipos de descoberta

Uma descoberta é uma notificação GuardDuty gerada quando detecta uma indicação de uma atividade suspeita ou maliciosa em sua Conta da AWS. GuardDuty gera uma descoberta em uma conta que foi ativada GuardDuty.

Para obter informações sobre mudanças importantes nos tipos de GuardDuty descoberta, incluindo tipos de descoberta recém-adicionados ou retirados, consulteHistórico de documentos da Amazon GuardDuty.

Para obter informações sobre os tipos de busca que agora estão desabilitados, consulte Tipos de descoberta desabilitados.

GuardDuty Tipos de descoberta do EC2

As descobertas a seguir são específicas dos recursos do Amazon EC2 e sempre têm um tipo de recurso `Instance`. A gravidade e os detalhes das descobertas serão diferentes com base na função de recurso, que indicará se a instância do EC2 foi alvo de atividade suspeita ou o agente que executou a atividade.

As descobertas listadas aqui incluem as fontes de dados e os modelos usados para gerar esse tipo de descoberta. Para obter mais informações sobre modelos e fontes de dados, consulte GuardDuty fontes de dados fundamentais.

> Observações
>
> - Detalhes da instância da descoberta do EC2 podem estar ausentes se a instância já tiver sido encerrada ou se a chamada de API subjacente tiver sido originada de uma instância do EC2 em uma região diferente.
> - As descobertas do EC2 que usam logs de fluxo da VPC como fonte de dados não oferecem suporte ao tráfego IPv6.

Para todas as descobertas do EC2, recomenda-se examinar o recurso em questão para determinar se ele está se comportando da maneira esperada. Se a atividade for autorizada, você poderá usar regras de supressão ou listas de IP confiáveis para evitar notificações de falsos positivos para esse recurso. Se a atividade for inesperada, a melhor prática de segurança será presumir que a instância

foi comprometida e executar as ações detalhadas em Como corrigir uma instância do Amazon EC2 potencialmente comprometida.

Tópicos

- Backdoor:EC2/C&CActivity.B
- Backdoor:EC2/C&CActivity.B!DNS
- Backdoor:EC2/DenialOfService.Dns
- Backdoor:EC2/DenialOfService.Tcp
- Backdoor:EC2/DenialOfService.Udp
- Backdoor:EC2/DenialOfService.UdpOnTcpPorts
- Backdoor:EC2/DenialOfService.UnusualProtocol
- Backdoor:EC2/Spambot
- Behavior:EC2/NetworkPortUnusual
- Behavior:EC2/TrafficVolumeUnusual
- CryptoCurrency:EC2/BitcoinTool.B
- CryptoCurrency:EC2/BitcoinTool.B!DNS
- DefenseEvasion:EC2/UnusualDNSResolver
- DefenseEvasion:EC2/UnusualDoHActivity
- DefenseEvasion:EC2/UnusualDoTActivity
- Impact:EC2/AbusedDomainRequest.Reputation
- Impact:EC2/BitcoinDomainRequest.Reputation
- Impact:EC2/MaliciousDomainRequest.Reputation
- Impact:EC2/MaliciousDomainRequest.Custom
- Impact:EC2/PortSweep
- Impact:EC2/SuspiciousDomainRequest.Reputation
- Impact:EC2/WinRMBruteForce
- Recon:EC2/PortProbeEMRUnprotectedPort
- Recon:EC2/PortProbeUnprotectedPort
- Recon:EC2/Portscan
- Trojan:EC2/BlackholeTraffic
- Trojan:EC2/BlackholeTraffic!DNS

- Trojan:EC2/DGADomainRequest.B
- Trojan:EC2/DGADomainRequest.C!DNS
- Trojan:EC2/DNSDataExfiltration
- Trojan:EC2/DriveBySourceTraffic!DNS
- Trojan:EC2/DropPoint
- Trojan:EC2/DropPoint!DNS
- Trojan:EC2/PhishingDomainRequest!DNS
- UnauthorizedAccess:EC2/MaliciousIPCaller.Custom
- UnauthorizedAccess:EC2/MetadataDNSRebind
- UnauthorizedAccess:EC2/RDPBruteForce
- UnauthorizedAccess:EC2/SSHBruteForce
- UnauthorizedAccess:EC2/TorClient
- UnauthorizedAccess:EC2/TorRelay

Backdoor:EC2/C&CActivity.B

A instância do EC2 está consultando um IP associado a um servidor de controle e comando conhecido.

Gravidade padrão: alta

- Fonte de dados: logs de fluxo da VPC

Essa descoberta informa que a instância listada em seu ambiente da AWS está consultando um IP associado a um servidor de comando e controle (C&C) conhecido. A instância listada pode estar comprometida. Os servidores de comando e controle são computadores que enviam comandos para membros de um botnet.

Um botnet é uma coleção de dispositivos conectados à Internet, que podem incluir PCs, servidores, dispositivos móveis e dispositivos de Internet das Coisas, infectados e controlados por um tipo comum de malware. Os botnets são frequentemente usados para distribuir malwares e coletar informações inapropriadas, como números de cartão de crédito. Dependendo da finalidade e da estrutura do botnet, o servidor de C&C também pode emitir comandos para iniciar um ataque de negação de serviço distribuída (DDoS).

> **Note**
>
> Se o IP consultado estiver relacionado ao log4j, os campos da descoberta associada incluirão estes valores:
>
> - service.additional = Amazon Info.threatListName
> - service.additional Info.threatName = Relacionado ao Log4j

Recomendações de correção:

Se essa atividade for inesperada, sua instância pode estar comprometida. Para obter mais informações, consulte Como corrigir uma instância do Amazon EC2 potencialmente comprometida.

Backdoor:EC2/C&CActivity.B!DNS

A instância do EC2 está consultando um nome de domínio associado a um servidor de controle e comando conhecido.

Gravidade padrão: alta

- Fonte de dados: logs de DNS

Essa descoberta informa que a instância listada em seu ambiente da AWS está consultando um nome de domínio associado a um servidor de comando e controle (C&C) conhecido. A instância listada pode estar comprometida. Os servidores de comando e controle são computadores que enviam comandos para membros de um botnet.

Um botnet é uma coleção de dispositivos conectados à Internet, que podem incluir PCs, servidores, dispositivos móveis e dispositivos de Internet das Coisas, infectados e controlados por um tipo comum de malware. Os botnets são frequentemente usados para distribuir malwares e coletar informações inapropriadas, como números de cartão de crédito. Dependendo da finalidade e da estrutura do botnet, o servidor de C&C também pode emitir comandos para iniciar um ataque de negação de serviço distribuída (DDoS).

> **Note**
>
> Se o nome de domínio consultado estiver relacionado ao log4j, os campos da descoberta associada incluirão os seguintes valores:

- service.additional = Amazon Info.threatListName
- service.additional Info.threatName = Relacionado ao Log4j

> **Note**
>
> Para testar como GuardDuty gera esse tipo de descoberta, você pode fazer uma solicitação de DNS da sua instância (usando `dig` para Linux ou `nslookup` Windows) em um domínio `guarddutyc2activityb.com` de teste.

Recomendações de correção:

Se essa atividade for inesperada, sua instância pode estar comprometida. Para obter mais informações, consulte Como corrigir uma instância do Amazon EC2 potencialmente comprometida.

Backdoor:EC2/DenialOfService.Dns

Uma instância do EC2 está se comportando de uma forma que pode indicar que está sendo usada para executar um ataque de negação de serviço (DoS) usando o protocolo DNS.

Gravidade padrão: alta

- Fonte de dados: logs de fluxo da VPC

Essa descoberta informa que a instância do EC2 listada em seu ambiente da AWS está gerando um grande volume de tráfego DNS de saída. Isso pode indicar que a instância está comprometida e está sendo usada para executar ataques de negação de serviço (DoS) usando o protocolo DNS.

> **Note**
>
> Essa descoberta detecta ataques de DoS somente contra endereços IP publicamente roteáveis, que são os principais alvos desses ataques.

Recomendações de correção:

Se essa atividade for inesperada, sua instância pode estar comprometida. Para obter mais informações, consulte Como corrigir uma instância do Amazon EC2 potencialmente comprometida.

Backdoor:EC2/DenialOfService.Tcp

Uma instância do EC2 está se comportando de uma forma que indica que ela está sendo usada para executar um ataque de negação de serviço (DoS – Denial of Service) usando o protocolo TCP.

Gravidade padrão: alta

- Fonte de dados: logs de fluxo da VPC

Essa descoberta informa que a instância do EC2 listada em seu ambiente da AWS está gerando um grande volume de tráfego TCP de saída. Isso pode indicar que a instância está comprometida e está sendo usada para executar ataques de negação de serviço (DoS) usando o protocolo TCP.

> **Note**
>
> Essa descoberta detecta ataques de DoS somente contra endereços IP publicamente roteáveis, que são os principais alvos desses ataques.

Recomendações de correção:

Se essa atividade for inesperada, sua instância pode estar comprometida. Para obter mais informações, consulte Como corrigir uma instância do Amazon EC2 potencialmente comprometida.

Backdoor:EC2/DenialOfService.Udp

Uma instância do EC2 está se comportando de uma forma que indica que ela está sendo usada para executar um ataque de negação de serviço (DoS) usando o protocolo UDP.

Gravidade padrão: alta

- Fonte de dados: logs de fluxo da VPC

Essa descoberta informa que a instância do EC2 listada em seu ambiente da AWS está gerando um grande volume de tráfego UDP de saída. Isso pode indicar que a instância está comprometida e está sendo usada para executar ataques de negação de serviço (DoS) usando o protocolo UDP.

> **Note**
>
> Essa descoberta detecta ataques de DoS somente contra endereços IP publicamente roteáveis, que são os principais alvos desses ataques.

Recomendações de correção:

Se essa atividade for inesperada, sua instância pode estar comprometida. Para obter mais informações, consulte Como corrigir uma instância do Amazon EC2 potencialmente comprometida.

Backdoor:EC2/DenialOfService.UdpOnTcpPorts

Uma instância do EC2 está se comportando de uma forma que pode indicar que está sendo usada para executar um ataque de negação de serviço (DoS) usando o protocolo UDP em uma porta TCP.

Gravidade padrão: alta

- Fonte de dados: logs de fluxo da VPC

Essa descoberta informa que a instância do EC2 listada em seu ambiente da AWS está gerando um grande volume de tráfego UDP de saída direcionado a uma porta que normalmente é usada para comunicação TCP. Isso pode indicar que a instância listada está comprometida e sendo usada para executar ataques de negação de serviço (DoS) usando o protocolo UDP em uma porta TCP.

> **Note**
>
> Essa descoberta detecta ataques de DoS somente contra endereços IP publicamente roteáveis, que são os principais alvos desses ataques.

Recomendações de correção:

Se essa atividade for inesperada, sua instância pode estar comprometida. Para obter mais informações, consulte Como corrigir uma instância do Amazon EC2 potencialmente comprometida.

Backdoor:EC2/DenialOfService.UnusualProtocol

Uma instância do EC2 está se comportando de uma forma que pode indicar que está sendo usada para executar um ataque de negação de serviço (DoS) usando um protocolo incomum.

Gravidade padrão: alta

- Fonte de dados: logs de fluxo da VPC

Essa descoberta informa que a instância do EC2 listada no seu ambiente da AWS está gerando um grande volume de tráfego de saída de um tipo de protocolo incomum que não é normalmente usado por instâncias do EC2, como Internet Group Management Protocol. Isso pode indicar que a instância está comprometida e está sendo usada para executar ataques de negação de serviço (DoS) usando um protocolo incomum. Essa descoberta detecta ataques de DoS somente contra endereços IP publicamente roteáveis, que são os principais alvos desses ataques.

Recomendações de correção:

Se essa atividade for inesperada, sua instância pode estar comprometida. Para obter mais informações, consulte Como corrigir uma instância do Amazon EC2 potencialmente comprometida.

Backdoor:EC2/Spambot

A instância do EC2 está exibindo um comportamento incomum ao se comunicar com um host remoto na porta 25.

Gravidade padrão: média

- Fonte de dados: logs de fluxo da VPC

Essa descoberta informa que a instância do EC2 listada em seu ambiente da AWS está se comunicando com um host remoto na porta 25. Esse comportamento é incomum, pois essa instância do EC2 não tem histórico prévio de comunicações com a porta 25. A porta 25 costuma ser usada por servidores de e-mail para comunicações SMTP. Essa descoberta indica que a instância do EC2 pode estar comprometida para uso por estar enviando spam.

Recomendações de correção:

Se essa atividade for inesperada, sua instância pode estar comprometida. Para obter mais informações, consulte Como corrigir uma instância do Amazon EC2 potencialmente comprometida.

Behavior:EC2/NetworkPortUnusual

Uma instância do EC2 está se comunicando com um host remoto em uma porta de servidor incomum.

Gravidade padrão: média

- Fonte de dados: logs de fluxo da VPC

Essa descoberta informa que a instância do EC2 listada em seu ambiente da AWS está se comportando de uma forma que se desvia da linha de base estabelecida. Essa instância do EC2 não tem histórico prévio de comunicações com essa porta remota.

> **Note**
>
> Se a instância do EC2 se comunicar na porta 389 ou na porta 1389, a gravidade da descoberta associada será modificada para Alta e os campos de descoberta incluirão o seguinte valor:
>
> - service.additional Info.context = Possível retorno de chamada log4j

Recomendações de correção:

Se essa atividade for inesperada, sua instância pode estar comprometida. Para obter mais informações, consulte Como corrigir uma instância do Amazon EC2 potencialmente comprometida.

Behavior:EC2/TrafficVolumeUnusual

A instância do EC2 está gerando quantidades grandes incomuns de tráfego de rede para um host remoto.

Gravidade padrão: média

- Fonte de dados: logs de fluxo da VPC

Essa descoberta informa que a instância do EC2 listada em seu ambiente da AWS está se comportando de uma forma que se desvia da linha de base estabelecida. Esta instância do EC2 não tem histórico prévio de enviar tanto tráfego assim para esse host remoto.

Recomendações de correção:

Se essa atividade for inesperada, sua instância pode estar comprometida. Para obter mais informações, consulte Como corrigir uma instância do Amazon EC2 potencialmente comprometida.

CryptoCurrency:EC2/BitcoinTool.B

Uma instância do EC2 está consultando um endereço IP associado à atividade relacionada à criptomoeda.

Gravidade padrão: alta

- Fonte de dados: logs de fluxo da VPC

Essa descoberta informa que a instância do EC2 listada em seu ambiente da AWS está consultando um endereço IP associado ao Bitcoin ou a outras atividades relacionadas a criptomoedas. O Bitcoin é uma criptomoeda mundial e um sistema de pagamento digital que pode ser trocado por outras moedas, produtos e serviços. O Bitcoin é uma recompensa pela mineração de bitcoins e é muito procurado por agentes de ameaças.

Recomendações de correção:

Se você usar essa instância do EC2 para minerar ou gerenciar criptomoeda ou se essa instância estiver envolvida de outra forma na atividade de blockchain, essa descoberta poderia representar a atividade esperada para o ambiente. Se esse for o caso em seu ambiente da AWS , recomendamos configurar uma regra de supressão para essa descoberta. A regra de supressão deve consistir em dois critérios de filtro. O primeiro critério deve usar o atributo Tipo de descoberta com um valor de `CryptoCurrency:EC2/BitcoinTool.B`. O segundo critério de filtro deve ser o ID de instância da instância envolvida na atividade de blockchain. Para saber mais sobre a criação de regras de supressão, consulte Regras de supressão em GuardDuty.

Se essa atividade for inesperada, sua instância provavelmente está comprometida. Consulte Como corrigir uma instância do Amazon EC2 potencialmente comprometida.

CryptoCurrency:EC2/BitcoinTool.B!DNS

Uma instância do EC2 está consultando um nome de domínio associado à atividade relacionada à criptomoeda.

Gravidade padrão: alta

- Fonte de dados: logs de DNS

Essa descoberta informa que a instância do EC2 listada em seu ambiente da AWS está consultando um nome de domínio associado ao Bitcoin ou a outras atividades relacionadas a criptomoedas. O Bitcoin é uma criptomoeda mundial e um sistema de pagamento digital que pode ser trocado por outras moedas, produtos e serviços. O Bitcoin é uma recompensa pela mineração de bitcoins e é muito procurado por agentes de ameaças.

Recomendações de correção:

Se você usar essa instância do EC2 para minerar ou gerenciar criptomoeda ou se essa instância estiver envolvida de outra forma na atividade de blockchain, essa descoberta poderia representar a atividade esperada para o ambiente. Se esse for o caso em seu ambiente da AWS , recomendamos configurar uma regra de supressão para essa descoberta. A regra de supressão deve consistir em dois critérios de filtro. O primeiro critério deve usar o atributo Tipo de descoberta com um valor de `CryptoCurrency:EC2/BitcoinTool.B!DNS`. O segundo critério de filtro deve ser o ID de instância da instância envolvida na atividade de blockchain. Para saber mais sobre a criação de regras de supressão, consulte Regras de supressão em GuardDuty.

Se essa atividade for inesperada, sua instância provavelmente está comprometida. Consulte Como corrigir uma instância do Amazon EC2 potencialmente comprometida.

DefenseEvasion:EC2/UnusualDNSResolver

Uma instância do Amazon EC2 está se comunicando com um resolvedor de DNS público incomum.

Gravidade padrão: média

- Fonte de dados: logs de fluxo da VPC

Essa descoberta informa que a instância do Amazon EC2 listada em seu ambiente da AWS está se comportando de uma forma que se desvia do comportamento da linha de base. Essa instância do EC2 não tem histórico recente de comunicação com esse resolvedor de DNS público. O campo Incomum no painel de detalhes da descoberta no GuardDuty console pode fornecer informações sobre o resolvedor de DNS consultado.

Recomendações de correção:

Se essa atividade for inesperada, sua instância pode estar comprometida. Para obter mais informações, consulte Como corrigir uma instância do Amazon EC2 potencialmente comprometida.

DefenseEvasion:EC2/UnusualDoHActivity

Uma instância do Amazon EC2 está executando uma comunicação incomum de DNS sobre HTTPS (DoH).

Gravidade padrão: média

- Fonte de dados: logs de fluxo da VPC

Essa descoberta informa que a instância do Amazon EC2 listada em seu ambiente da AWS está se comportando de uma forma que se desvia da linha de base estabelecida. Essa instância do EC2 não tem histórico recente de comunicações de DNS sobre HTTPS (DoH) com esse servidor público do DoH. Nos detalhes da descoberta, o campo Incomum pode fornecer informações sobre o servidor DoH consultado.

Recomendações de correção:

Se essa atividade for inesperada, sua instância pode estar comprometida. Para obter mais informações, consulte Como corrigir uma instância do Amazon EC2 potencialmente comprometida.

DefenseEvasion:EC2/UnusualDoTActivity

Uma instância do Amazon EC2 está executando uma comunicação incomum de DNS sobre TLS (DoT).

Gravidade padrão: média

- Fonte de dados: logs de fluxo da VPC

Essa descoberta informa que a instância do EC2 listada em seu ambiente da AWS está se comportando de uma forma que se desvia da linha de base estabelecida. Essa instância do EC2 não tem histórico recente de comunicações de DNS sobre TLS (DoT) com esse servidor DoT público. No painel de detalhes da descoberta, o campo Incomum pode fornecer informações sobre o servidor DoT consultado.

Recomendações de correção:

Se essa atividade for inesperada, sua instância pode estar comprometida. Para obter mais informações, consulte Como corrigir uma instância do Amazon EC2 potencialmente comprometida.

Impact:EC2/AbusedDomainRequest.Reputation

Uma instância do EC2 está consultando um nome de domínio com baixa reputação associado a domínios conhecidos que permitem abusos.

Gravidade padrão: média

- Fonte de dados: logs de DNS

Essa descoberta informa que a instância do Amazon EC2 listada em seu ambiente da AWS está consultando um nome de domínio de baixa reputação associado a domínios ou endereços IP de abuso conhecidos. Exemplos de domínios abusados são nomes de domínio de nível superior (TLDs) e nomes de domínio de segundo nível (2LDs) que fornecem registros gratuitos de subdomínios, bem como provedores de DNS dinâmicos. Os agentes de ameaças tendem a usar esses serviços para registrar domínios gratuitamente ou a baixo custo. Os domínios de baixa reputação nessa categoria também podem ser domínios expirados que se resolvem para o endereço IP estacionário de um registrador e, portanto, podem não estar mais ativas. Um IP de estacionamento é onde um registrador direciona o tráfego para domínios que não foram vinculados a nenhum serviço. É possível que a instância listada do Amazon EC2 esteja comprometida, pois os agentes de ameaças geralmente usam esses registradores ou serviços para C&C e distribuição de malware.

Os domínios de baixa reputação são baseados em um modelo de pontuação de reputação. Esse modelo avalia e classifica as características de um domínio para determinar sua probabilidade de ser mal-intencionado.

Recomendações de correção:

Se essa atividade for inesperada, sua instância pode estar comprometida. Para obter mais informações, consulte Como corrigir uma instância do Amazon EC2 potencialmente comprometida.

Impact:EC2/BitcoinDomainRequest.Reputation

Uma instância do EC2 está consultando um nome de domínio associado à atividade relacionada à criptomoeda.

Gravidade padrão: alta

- Fonte de dados: logs de DNS

Essa descoberta informa que a instância do Amazon EC2 listada em seu ambiente da AWS está consultando um nome de domínio de baixa reputação associado ao Bitcoin ou a outras atividades relacionadas a criptomoedas. O Bitcoin é uma criptomoeda mundial e um sistema de pagamento digital que pode ser trocado por outras moedas, produtos e serviços. O Bitcoin é uma recompensa pela mineração de bitcoins e é muito procurado por agentes de ameaças.

Os domínios de baixa reputação são baseados em um modelo de pontuação de reputação. Esse modelo avalia e classifica as características de um domínio para determinar sua probabilidade de ser mal-intencionado.

Recomendações de correção:

Se você usar essa instância do EC2 para minerar ou gerenciar criptomoeda ou se essa instância estiver envolvida de outra forma na atividade de blockchain, essa descoberta poderia representar a atividade esperada para o ambiente. Se esse for o caso em seu ambiente da AWS , recomendamos configurar uma regra de supressão para essa descoberta. A regra de supressão deve consistir em dois critérios de filtro. O primeiro critério deve usar o atributo Tipo de descoberta com um valor de `Impact:EC2/BitcoinDomainRequest.Reputation`. O segundo critério de filtro deve ser o ID de instância da instância envolvida na atividade de blockchain. Para saber mais sobre a criação de regras de supressão, consulte Regras de supressão em GuardDuty.

Se essa atividade for inesperada, sua instância provavelmente está comprometida. Consulte Como corrigir uma instância do Amazon EC2 potencialmente comprometida.

Impact:EC2/MaliciousDomainRequest.Reputation

Uma instância do EC2 está consultando um domínio de baixa reputação associado a domínios mal-intencionados conhecidos.

Gravidade padrão: alta

- Fonte de dados: logs de DNS

Essa descoberta informa que a instância do Amazon EC2 listada em seu ambiente da AWS está consultando um nome de domínio de baixa reputação associado a domínios ou endereços IP mal-intencionados conhecidos. Por exemplo, os domínios podem estar associados a um endereço IP sumidouro conhecido. Domínios sinkholed são domínios que antes eram controlados por um agente de ameaças, e as solicitações feitas a eles podem indicar que a instância está comprometida. Esses domínios também podem estar correlacionados com campanhas mal-intencionadas conhecidas ou algoritmos de geração de domínio.

Os domínios de baixa reputação são baseados em um modelo de pontuação de reputação. Esse modelo avalia e classifica as características de um domínio para determinar sua probabilidade de ser mal-intencionado.

Recomendações de correção:

Se essa atividade for inesperada, sua instância pode estar comprometida. Para obter mais informações, consulte Como corrigir uma instância do Amazon EC2 potencialmente comprometida.

Impact:EC2/MaliciousDomainRequest.Custom

Uma instância do EC2 está consultando um domínio em uma lista de entidades de ameaça personalizada.

Gravidade padrão: média

- Fonte de dados: logs de DNS

Essa descoberta informa que a instância do Amazon EC2 listada em seu ambiente da AWS está consultando um nome de domínio incluído na lista de entidades de ameaças que você carregou e ativou. Em GuardDuty, uma lista de entidades de ameaça consiste em nomes de domínio e endereços IP maliciosos conhecidos. GuardDuty gera descobertas com base na atividade associada à lista de entidades ameaçadoras carregada. É possível visualizar o nome dessa lista de entidades de ameaças nos detalhes da descoberta.

Recomendações de correção:

Se essa atividade for inesperada, sua instância pode estar comprometida. Para obter mais informações, consulte Como corrigir uma instância do Amazon EC2 potencialmente comprometida.

Impact:EC2/PortSweep

Uma instância do EC2 está testando uma porta em um muitos endereços IP.

Gravidade padrão: alta

- Fonte de dados: logs de fluxo da VPC

Essa descoberta informa que a instância do EC2 listada em seu AWS ambiente está testando uma porta em um grande número de endereços IP roteáveis publicamente. Esse tipo de atividade geralmente é usado para encontrar hospedeiros vulneráveis para serem explorados. No painel de detalhes de busca em seu GuardDuty console, somente o endereço IP remoto mais recente é exibido

Recomendações de correção:

Se essa atividade for inesperada, sua instância pode estar comprometida. Para obter mais informações, consulte Como corrigir uma instância do Amazon EC2 potencialmente comprometida.

Impact:EC2/SuspiciousDomainRequest.Reputation

Uma instância do EC2 está consultando um nome de domínio com baixa reputação que é suspeito por natureza devido à sua idade ou baixa popularidade.

Gravidade padrão: baixa

- Fonte de dados: logs de DNS

Essa descoberta informa que a instância do Amazon EC2 listada em seu ambiente da AWS está consultando um nome de domínio com baixa reputação que é suspeito de ser mal-intencionado. Foram percebidas características desse domínio que eram consistentes com domínios mal-intencionados observados anteriormente. No entanto, nosso modelo de reputação não conseguiu relacioná-lo definitivamente a uma ameaça conhecida. Esses domínios geralmente são observados recentemente ou recebem uma quantidade baixa de tráfego.

Os domínios de baixa reputação são baseados em um modelo de pontuação de reputação. Esse modelo avalia e classifica as características de um domínio para determinar sua probabilidade de ser mal-intencionado.

Recomendações de correção:

Se essa atividade for inesperada, sua instância pode estar comprometida. Para obter mais informações, consulte Como corrigir uma instância do Amazon EC2 potencialmente comprometida.

Impact:EC2/WinRMBruteForce

Uma instância do EC2 está executando um ataque de força bruta de saída do Gerenciamento Remoto do Windows.

Gravidade padrão: baixa*

> **Note**
>
> A gravidade dessa descoberta é baixa se a instância do EC2 foi o alvo de um ataque de força bruta. A gravidade dessa descoberta será alta se sua instância do EC2 for o agente que está sendo usado para executar o ataque de força bruta.

- Fonte de dados: logs de fluxo da VPC

Essa descoberta informa que a instância do EC2 listada em seu AWS ambiente está executando um ataque de força bruta do Windows Remote Management (WinRM) com o objetivo de obter acesso ao serviço de Gerenciamento Remoto do Windows nos sistemas. Windows-based

Recomendações de correção:

Se essa atividade for inesperada, sua instância pode estar comprometida. Para obter mais informações, consulte Como corrigir uma instância do Amazon EC2 potencialmente comprometida.

Recon:EC2/PortProbeEMRUnprotectedPort

Uma instância do EC2 tem uma porta relacionada ao EMR desprotegida que está sendo testada por um host mal-intencionado conhecido.

Gravidade padrão: alta

- Fonte de dados: logs de fluxo da VPC

Essa descoberta informa que uma porta confidencial relacionada ao EMR na instância EC2 listada que faz parte de um cluster em AWS seu ambiente não está bloqueada por um grupo de segurança,

uma lista de controle de acesso (ACL) ou um firewall no host, como Linux IPTables. Essa descoberta também informa que verificadores conhecidos na Internet examinam ativamente essa porta. Portas que podem acionar essa descoberta, como a porta 8088 (porta da IU da Web do YARN), possivelmente podem ser usadas para execução de código remoto.

Recomendações de correção:

Você deve bloquear o acesso a portas abertas nos clusters pela Internet e restringir o acesso apenas a endereços IP específicos que exigem acesso a essas portas. Para obter mais informações, consulte Grupos de segurança para a clusters do EMR.

Recon:EC2/PortProbeUnprotectedPort

Uma instância do EC2 tem uma porta desprotegida que está sendo testada por um host mal-intencionado conhecido.

Gravidade padrão: baixa*

> **Note**
>
> A gravidade padrão dessa descoberta é baixa. No entanto, se a porta que está sendo sondada for usada pelo Elasticsearch (9200 ou 9300), a severidade da descoberta será alta.

- Fonte de dados: logs de fluxo da VPC

Essa descoberta informa que uma porta na instância do EC2 listada em seu ambiente da AWS não está bloqueada por um grupo de segurança, uma lista de controle de acesso (ACL) ou um firewall no host, como o IPTables do Linux, e que scanners conhecidos na Internet estão sondando-a ativamente.

Se a porta desprotegida identificada for 22 ou 3389 e você estiver usando essas portas para se conectar à instância, ainda será possível limitar a exposição permitindo o acesso a essas portas somente aos endereços IP do espaço de endereços IP da rede corporativa. Para restringir o acesso à porta 22 no Linux, consulte Autorizar o tráfego de entrada para suas instâncias do Linux. Para restringir o acesso à porta 3389 no Windows, consulte Autorizar o tráfego de entrada para suas instâncias do Windows.

GuardDuty não gera essa descoberta para as portas 443 e 80.

Recomendações de correção:

Pode haver casos em que as instâncias são intencionalmente expostas; por exemplo, se estiverem hospedando servidores web. Se esse for o caso em seu AWS ambiente, recomendamos que você configure uma regra de supressão para essa descoberta. A regra de supressão deve consistir em dois critérios de filtro. O primeiro critério deve usar o atributo Tipo de descoberta com um valor de `Recon:EC2/PortProbeUnprotectedPort`. O segundo critério de filtro deve corresponder a uma ou mais instâncias que servem como um bastion host. É possível usar o atributo ID da imagem da instância ou o atributo de valor da Tag dependendo de quais critérios forem identificáveis com as instâncias que hospedam essas ferramentas. Para obter mais informações sobre como criar regras de supressão, consulte Regras de supressão em GuardDuty.

Se essa atividade for inesperada, sua instância provavelmente está comprometida. Consulte Como corrigir uma instância do Amazon EC2 potencialmente comprometida.

Recon:EC2/Portscan

Uma instância do EC2 está executando verificações de portas de saída para um host remoto.

Gravidade padrão: média

- Fonte de dados: logs de fluxo da VPC

Essa descoberta informa que a instância do EC2 listada em seu ambiente da AWS está envolvida em um possível ataque de varredura de porta porque está tentando se conectar a várias portas em um curto período de tempo. O objetivo de um ataque de verificação de porta é localizar portas abertas para descobrir quais serviços a máquina está executando e identificar o sistema operacional dela.

Recomendações de correção:

Essa descoberta pode ser um falso positivo quando aplicativas de avaliação de vulnerabilidade são implantados em instâncias do EC2 no ambiente, pois esses aplicativas realizam verificações de portas para alertar sobre portas abertas configuradas incorretamente. Se esse for o caso em seu AWS ambiente, recomendamos que você configure uma regra de supressão para essa descoberta. A regra de supressão deve consistir em dois critérios de filtro. O primeiro critério deve usar o atributo Tipo de descoberta com um valor de `Recon:EC2/Portscan`. O segundo critério de filtro deve corresponder a uma ou mais instâncias que hospedam essas ferramentas de avaliação de

vulnerabilidade. É possível usar o atributo ID da imagem da instância ou o atributo de valor da Tag dependendo de quais critérios forem identificáveis com as instâncias que hospedam essas ferramentas. Para obter mais informações sobre como criar regras de supressão, consulte Regras de supressão em GuardDuty.

Se essa atividade for inesperada, sua instância provavelmente está comprometida. Consulte Como corrigir uma instância do Amazon EC2 potencialmente comprometida.

Trojan:EC2/BlackholeTraffic

Uma instância do EC2 está tentando se comunicar com um endereço IP de um host remoto que é um buraco negro conhecido.

Gravidade padrão: média

- Fonte de dados: logs de fluxo da VPC

Essa descoberta informa que a instância EC2 listada em seu AWS ambiente pode estar comprometida porque está tentando se comunicar com o endereço IP de um buraco negro (ou sumidouro). Buracos negros são lugares na rede em que o tráfego de entrada ou saída é descartado silenciosamente sem informar à fonte que os dados não chegaram ao destinatário pretendido. Um endereço IP de buraco negro especifica uma máquina host que não está sendo executada ou um endereço para o qual nenhum host foi atribuído.

Recomendações de correção:

Se essa atividade for inesperada, sua instância pode estar comprometida. Para obter mais informações, consulte Como corrigir uma instância do Amazon EC2 potencialmente comprometida.

Trojan:EC2/BlackholeTraffic!DNS

Uma instância do EC2 está consultando um nome de domínio que está sendo redirecionado para o endereço IP de um buraco negro.

Gravidade padrão: média

- Fonte de dados: logs de DNS

Essa descoberta informa que a instância EC2 listada em seu AWS ambiente pode estar comprometida porque está consultando um nome de domínio que está sendo redirecionado para um endereço IP de buraco negro. Buracos negros são lugares na rede em que o tráfego de entrada ou saída é descartado silenciosamente sem informar à fonte que os dados não chegaram ao destinatário pretendido.

Recomendações de correção:

Se essa atividade for inesperada, sua instância pode estar comprometida. Para obter mais informações, consulte Como corrigir uma instância do Amazon EC2 potencialmente comprometida.

Trojan:EC2/DGADomainRequest.B

Uma instância do EC2 está consultando domínios gerados por algoritmos. Esses domínios são comumente usados por malware e podem ser um indicativo de uma instância do EC2 comprometida.

Gravidade padrão: alta

- Fonte de dados: logs de DNS

Essa descoberta informa que a instância do EC2 listada no seu ambiente da AWS está tentando consultar domínios do algoritmo de geração de domínio (DGA). Sua instância do EC2 pode estar comprometida.

Os DGAs são usados para gerar periodicamente uma grande quantidade de nomes de domínio que podem ser usados como pontos de encontro com seus servidores de comando e controle (C&C). Os servidores de comando e controle são computadores que emitem comandos para membros de um botnet, ou seja, uma coleção de dispositivos conectados à Internet infectados e controlados por um tipo comum de malware. Quando há um grande número de possíveis pontos de encontro, isso dificulta o encerramento efetivo dos botnets, uma vez que os computadores infectados tentam entrar em contato com alguns desses nomes de domínio todos os dias para receber atualizações ou comandos.

> **Note**
>
> Essa descoberta é baseada na análise de nomes de domínio usando heurística avançada e pode identificar novos domínios de DGA que não estão presentes em feeds de inteligência contra ameaças.

Recomendações de correção:

Se essa atividade for inesperada, sua instância pode estar comprometida. Para obter mais informações, consulte Como corrigir uma instância do Amazon EC2 potencialmente comprometida.

Trojan:EC2/DGADomainRequest.C!DNS

Uma instância do EC2 está consultando domínios gerados por algoritmos. Esses domínios são comumente usados por malware e podem ser um indicativo de uma instância do EC2 comprometida.

Gravidade padrão: alta

- Fonte de dados: logs de DNS

Essa descoberta informa que a instância do EC2 listada no seu ambiente da AWS está tentando consultar domínios do algoritmo de geração de domínio (DGA). Sua instância do EC2 pode estar comprometida.

Os DGAs são usados para gerar periodicamente uma grande quantidade de nomes de domínio que podem ser usados como pontos de encontro com seus servidores de comando e controle (C&C). Os servidores de comando e controle são computadores que emitem comandos para membros de um botnet, ou seja, uma coleção de dispositivos conectados à Internet infectados e controlados por um tipo comum de malware. Quando há um grande número de possíveis pontos de encontro, isso dificulta o encerramento efetivo dos botnets, uma vez que os computadores infectados tentam entrar em contato com alguns desses nomes de domínio todos os dias para receber atualizações ou comandos.

> **Note**
>
> Essa descoberta é baseada em domínios DGA conhecidos dos feeds de inteligência de ameaças GuardDuty da.

Recomendações de correção:

Se essa atividade for inesperada, sua instância pode estar comprometida. Para obter mais informações, consulte Como corrigir uma instância do Amazon EC2 potencialmente comprometida.

Trojan:EC2/DNSDataExfiltration

Uma instância do EC2 está exfiltrando dados por meio de consultas DNS.

Gravidade padrão: alta

- Fonte de dados: logs de DNS

Essa descoberta informa que a instância do EC2 listada em seu ambiente da AWS está executando um malware que usa consultas ao DNS para transferências de dados de saída. Esse tipo de transferência de dados é indicativo de uma instância comprometida e pode resultar na exfiltração de dados. Normalmente, o tráfego de DNS não é bloqueado por firewalls. Por exemplo, o malware em uma instância do EC2 comprometida pode codificar dados (p. ex., seu número de cartão de crédito) em uma consulta ao DNS e enviá-los a um servidor de DNS remoto controlado por um invasor.

Recomendações de correção:

Se essa atividade for inesperada, sua instância pode estar comprometida. Para obter mais informações, consulte Como corrigir uma instância do Amazon EC2 potencialmente comprometida.

Trojan:EC2/DriveBySourceTraffic!DNS

Uma instância do EC2 está consultando o nome de domínio de um host remoto que é uma fonte conhecida de ataques de Drive-By download.

Gravidade padrão: alta

- Fonte de dados: logs de DNS

Essa descoberta informa a você que uma instância do EC2 em seu ambiente da AWS pode estar comprometida porque está consultando um nome de domínio de um host remoto que é uma fonte conhecida de ataques Drive-by download. Estes são downloads indesejados de software de computador da Internet que podem acionar uma instalação automática de vírus, spyware ou malware.

Recomendações de correção:

Se essa atividade for inesperada, sua instância pode estar comprometida. Para obter mais informações, consulte Como corrigir uma instância do Amazon EC2 potencialmente comprometida.

Trojan:EC2/DropPoint

Uma instância do EC2 está tentando se comunicar com um endereço IP de um host remoto que é conhecido por manter credenciais e outros dados roubados capturados por malware.

Gravidade padrão: média

- Fonte de dados: logs de fluxo da VPC

Essa descoberta informa que uma instância do EC2 em seu AWS ambiente está tentando se comunicar com um endereço IP de um host remoto que é conhecido por conter credenciais e outros dados roubados capturados por malware.

Recomendações de correção:

Se essa atividade for inesperada, sua instância pode estar comprometida. Para obter mais informações, consulte Como corrigir uma instância do Amazon EC2 potencialmente comprometida.

Trojan:EC2/DropPoint!DNS

Uma instância do EC2 está consultando um nome de domínio de um host remoto que é conhecido por manter credenciais e outros dados roubados capturados por malware.

Gravidade padrão: média

- Fonte de dados: logs de DNS

Essa descoberta informa que uma instância do EC2 em seu AWS ambiente está consultando o nome de domínio de um host remoto que é conhecido por conter credenciais e outros dados roubados capturados por malware.

Recomendações de correção:

Se essa atividade for inesperada, sua instância pode estar comprometida. Para obter mais informações, consulte Como corrigir uma instância do Amazon EC2 potencialmente comprometida.

Trojan:EC2/PhishingDomainRequest!DNS

Uma instância do EC2 está consultando domínios envolvidos em ataques de phishing. Sua instância do EC2 pode estar comprometida.

Gravidade padrão: alta

- Fonte de dados: logs de DNS

Essa descoberta informa que existe uma instância do EC2 no seu ambiente da AWS que está tentando consultar um domínio envolvido em ataques de phishing. Domínios de phishing são configuradas por alguém se passando por uma instituição legítima para induzir indivíduos a fornecerem dados confidenciais, como informações de identificação pessoal, dados bancários e de cartão de crédito, e senhas. Sua instância do EC2 pode estar tentando recuperar dados confidenciais armazenados em um site de phishing ou configurar um site de phishing. Sua instância do EC2 pode estar comprometida.

Recomendações de correção:

Se essa atividade for inesperada, sua instância pode estar comprometida. Para obter mais informações, consulte Como corrigir uma instância do Amazon EC2 potencialmente comprometida.

UnauthorizedAccess:EC2/MaliciousIPCaller.Custom

Uma instância do EC2 está fazendo conexões com um endereço IP em uma lista de ameaças personalizada.

Gravidade padrão: média

- Fonte de dados: logs de fluxo da VPC

Essa descoberta informa que uma instância do EC2 em seu AWS ambiente está se comunicando com um endereço IP incluído em uma lista de ameaças que você enviou. Em GuardDuty, uma lista de ameaças consiste em endereços IP maliciosos conhecidos. GuardDuty gera descobertas com base em listas de ameaças enviadas. A lista de ameaças usada para gerar essa descoberta será indicada nos detalhes da descoberta.

Recomendações de correção:

Se essa atividade for inesperada, sua instância pode estar comprometida. Para obter mais informações, consulte Como corrigir uma instância do Amazon EC2 potencialmente comprometida.

UnauthorizedAccess:EC2/MetadataDNSRebind

Uma instância do EC2 está executando pesquisas de DNS que são resolvidas como o serviço de metadados da instância.

Gravidade padrão: alta

- Fonte de dados: logs de DNS

Essa descoberta informa que uma instância do EC2 em seu AWS ambiente está consultando um domínio que resolve para o endereço IP dos metadados do EC2 (169.254.169.254). Uma consulta ao DNS desse tipo pode indicar que a instância é alvo de uma técnica de revinculação de DNS. Essa técnica pode ser usada para obter metadados de uma instância do EC2, incluindo as credenciais do IAM associadas à instância.

A revinculação de DNS envolve enganar um aplicativo em execução na instância do EC2 para carregar dados de retorno de um URL, onde o nome de domínio no URL é resolvido como o endereço IP de metadados do EC2 (169.254.169.254). Isso faz com que a aplicação acesse metadados do EC2 e possivelmente os disponibilize para o invasor.

É possível acessar metadados do EC2 usando a revinculação de DNS somente se a instância do EC2 estiver executando um aplicativo vulnerável que permita a injeção de URLs ou se um usuário humano acessar a URL em um navegador da web em execução na instância do EC2.

Recomendações de correção:

Em resposta a essa descoberta, você deve avaliar se há um aplicativo vulnerável em execução na instância do EC2 ou se um usuário humano usou um navegador para acessar o domínio identificado

na descoberta. Se a causa raiz for uma aplicação vulnerável, você deverá corrigir a vulnerabilidade. Se alguém navegou pelo domínio identificado, você deve bloquear o domínio ou evitar que os usuários o acessem. Se você determinar que essa descoberta estava relacionada a qualquer um dos casos acima, deverá revogar a sessão associada à instância do EC2.

Alguns AWS clientes mapeiam intencionalmente o endereço IP dos metadados para um nome de domínio em seus servidores DNS autorizados. Se esse for o caso em seu ambiente da , recomendamos configurar uma regra de supressão para essa descoberta. A regra de supressão deve consistir em dois critérios de filtro. O primeiro critério deve usar o atributo Tipo de descoberta com um valor de `UnauthorizedAccess:EC2/MetaDataDNSRebind`. O segundo critério de filtro deve ser o domínio de solicitação de DNS e o valor deve corresponder ao domínio mapeado para o endereço IP de metadados (169.254.169.254). Para obter mais informações sobre como criar regras de supressão, consulte Regras de supressão em GuardDuty.

UnauthorizedAccess:EC2/RDPBruteForce

Uma instância do EC2 esteve envolvida em ataques de força bruta do RDP.

Gravidade padrão: baixa*

> **Note**
>
> A gravidade dessa descoberta é baixa se a instância do EC2 foi o alvo de um ataque de força bruta. A gravidade dessa descoberta será alta se sua instância do EC2 for o agente que está sendo usado para executar o ataque de força bruta.

- Fonte de dados: logs de fluxo da VPC

Essa descoberta informa que uma instância do EC2 em seu AWS ambiente estava envolvida em um ataque de força bruta com o objetivo de obter senhas para serviços RDP nos sistemas. Windows-based Isso pode indicar acesso não autorizado aos seus recursos da AWS .

Recomendações de correção:

Se a Função do recurso da instância é `ACTOR`, isso indica que a instância foi usada para executar ataques de força bruta RDP. A menos que essa instância tenha um motivo legítimo para entrar em contato com o endereço IP listado como o `Target`, é recomendável que você presuma que a

instância foi comprometida e execute as ações listadas em Como corrigir uma instância do Amazon EC2 potencialmente comprometida.

Se a Função do recurso da instância é `TARGET`, essa descoberta pode ser corrigida protegendo a porta RDP somente para IPs confiáveis por meio de grupos de segurança, ACLs ou firewalls. Para obter mais informações, consulte Dicas para proteger suas instâncias do EC2 (Linux).

UnauthorizedAccess:EC2/SSHBruteForce

Uma instância do EC2 esteve envolvida em ataques de força bruta do SSH.

Gravidade padrão: baixa*

> **Note**
>
> A gravidade dessa descoberta será baixa se um ataque de força bruta for destinado a uma de suas instâncias do EC2. A gravidade dessa descoberta será alta se sua instância do EC2 estiver sendo usada para executar o ataque de força bruta.

- Fonte de dados: logs de fluxo da VPC

Essa descoberta informa que uma instância do EC2 em seu AWS ambiente estava envolvida em um ataque de força bruta com o objetivo de obter senhas para serviços SSH nos sistemas. Linux-based Isso pode indicar acesso não autorizado aos seus recursos da AWS .

> **Note**
>
> Essa descoberta é gerada apenas por meio do monitoramento de tráfego do na porta 22. Se os serviços de SSH estiverem configurados para usar outras portas, essa descoberta não será gerada.

Recomendações de correção:

Se o alvo da tentativa de força bruta for um hospedeiro de bastião, isso pode representar o comportamento esperado para seu AWS ambiente. Se for esse o caso, recomendamos configurar uma regra de supressão para essa descoberta. A regra de supressão deve consistir em dois

critérios de filtro. O primeiro critério deve usar o atributo Tipo de descoberta com um valor de `UnauthorizedAccess:EC2/SSHBruteForce`. O segundo critério de filtro deve corresponder a uma ou mais instâncias que servem como um bastion host. É possível usar o atributo ID da imagem da instância ou o atributo de valor da Tag dependendo de quais critérios forem identificáveis com as instâncias que hospedam essas ferramentas. Para obter mais informações sobre como criar regras de supressão, consulte Regras de supressão em GuardDuty.

Se essa atividade não for esperada para o ambiente e a Função do recurso da instância for `TARGET`, essa descoberta poderá ser corrigida protegendo a porta SSH somente para IPs confiáveis por meio de grupos de segurança, ACLs ou firewalls. Para obter mais informações, consulte Dicas para proteger sua instância do EC2.

Se a Função do recurso da instância for `ACTOR` isso indicará que a instância foi usada para executar ataques de força bruta do SSH. A menos que essa instância tenha um motivo legítimo para entrar em contato com o endereço IP listado como o `Target`, é recomendável que você presuma que a instância foi comprometida e execute as ações listadas em Como corrigir uma instância do Amazon EC2 potencialmente comprometida.

UnauthorizedAccess:EC2/TorClient

A instância do EC2 está fazendo conexões com um Tor Guard ou um nó de autoridade.

Gravidade padrão: alta

- Fonte de dados: logs de fluxo da VPC

Essa descoberta informa que uma instância do EC2 em seu AWS ambiente está fazendo conexões com um Tor Guard ou um nó de Autoridade. Tor é um software para permitir a comunicação anônima. Tor Guards ou nós de autoridade atuam como gateways iniciais em uma rede do Tor. Esse tráfego pode indicar que a instância do EC2 foi comprometida está atuando como um cliente em uma rede do Tor. Essa descoberta pode indicar acesso não autorizado aos seus AWS recursos com a intenção de ocultar a verdadeira identidade do atacante.

Recomendações de correção:

Se essa atividade for inesperada, sua instância pode estar comprometida. Para obter mais informações, consulte Como corrigir uma instância do Amazon EC2 potencialmente comprometida.

UnauthorizedAccess:EC2/TorRelay

A instância do EC2 está fazendo conexões com uma rede do Tor como uma retransmissão Tor.

Gravidade padrão: alta

- Fonte de dados: logs de fluxo da VPC

Essa descoberta informa que uma instância do EC2 em seu AWS ambiente está fazendo conexões com uma rede Tor de uma maneira que sugere que ela está agindo como um retransmissor Tor. Tor é um software para permitir a comunicação anônima. Retransmissões Tor aumentam o anonimato da comunicação encaminhando o tráfego possivelmente ilícito do cliente de uma retransmissão Tor para outra.

Recomendações de correção:

Se essa atividade for inesperada, sua instância pode estar comprometida. Para obter mais informações, consulte Como corrigir uma instância do Amazon EC2 potencialmente comprometida.

GuardDuty Tipos de descoberta do IAM

As descobertas a seguir são específicas de entidades e chaves de acesso do IAM e sempre têm um Tipo de recurso igual a `AccessKey`. A gravidade e os detalhes das descobertas serão diferentes com base no tipo de descoberta.

As descobertas listadas aqui incluem as fontes de dados e os modelos usados para gerar esse tipo de descoberta. Para obter mais informações, consulte GuardDuty fontes de dados fundamentais.

Para todas as IAM-related descobertas, recomendamos que você examine a entidade em questão e garanta que suas permissões sigam a melhor prática de privilégio mínimo. Se essa atividade for inesperada, suas credenciais podem estar comprometidas. Consulte . Para obter mais informações sobre correção de descobertas, consulte Correção de problemas potencialmente comprometidos AWS credenciais.

Tópicos

- CredentialAccess:IAMUser/AnomalousBehavior
- CredentialAccess:IAMUser/CompromisedCredentials

- DefenseEvasion:IAMUser/AnomalousBehavior
- DefenseEvasion:IAMUser/BedrockLoggingDisabled
- Discovery:IAMUser/AnomalousBehavior
- Exfiltration:IAMUser/AnomalousBehavior
- Impact:IAMUser/AnomalousBehavior
- InitialAccess:IAMUser/AnomalousBehavior
- PenTest:IAMUser/KaliLinux
- PenTest:IAMUser/ParrotLinux
- PenTest:IAMUser/PentooLinux
- Persistence:IAMUser/AnomalousBehavior
- Policy:IAMUser/RootCredentialUsage
- Policy:IAMUser/ShortTermRootCredentialUsage
- PrivilegeEscalation:IAMUser/AnomalousBehavior
- Recon:IAMUser/MaliciousIPCaller
- Recon:IAMUser/MaliciousIPCaller.Custom
- Recon:IAMUser/TorIPCaller
- Stealth:IAMUser/CloudTrailLoggingDisabled
- Stealth:IAMUser/PasswordPolicyChange
- UnauthorizedAccess:IAMUser/ConsoleLoginSuccess.B
- UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.InsideAWS
- UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS
- UnauthorizedAccess:IAMUser/MaliciousIPCaller
- UnauthorizedAccess:IAMUser/MaliciousIPCaller.Custom
- UnauthorizedAccess:IAMUser/ResourceCredentialExfiltration.InsideAWS
- UnauthorizedAccess:IAMUser/ResourceCredentialExfiltration.OutsideAWS
- UnauthorizedAccess:IAMUser/TorIPCaller

CredentialAccess:IAMUser/AnomalousBehavior

Uma API usada para obter acesso a um AWS o ambiente foi invocado de forma anômala.

Gravidade padrão: média

- Fonte de dados: evento CloudTrail de gerenciamento

Essa descoberta informa que uma solicitação de API anômala foi observada em sua conta. Essa descoberta pode incluir uma única API ou uma série de solicitações de API relacionadas feitas nas proximidades por uma única identidade de usuário. Comumente, a API observada é associada ao estágio de acesso às credenciais de um ataque quando um adversário está tentando coletar senhas, nomes de usuário e chaves de acesso para seu ambiente. As APIs nesta categoria são `GetPasswordData`, `GetSecretValue`, `BatchGetSecretValue` e `GenerateDbAuthToken`.

Essa solicitação de API foi identificada como anômala pelo modelo de aprendizado GuardDuty de máquina (ML) de detecção de anomalias. O modelo de ML avalia todas as solicitações de API em sua conta e identifica eventos anômalos associados às técnicas usadas pelos adversários. O modelo de ML rastreia vários fatores da solicitação de API, como o usuário que fez a solicitação, o local de onde a solicitação foi feita e a API específica que foi solicitada. Os detalhes sobre quais fatores da solicitação de API são incomuns para a identidade do usuário que invocou a solicitação podem ser encontrados nos detalhes da descoberta.

Recomendações de correção:

Se essa atividade for inesperada, suas credenciais podem estar comprometidas. Para obter mais informações, consulte Correção de problemas potencialmente comprometidos AWS credenciais.

CredentialAccess:IAMUser/CompromisedCredentials

Uma chave de acesso do IAM foi identificada como potencialmente comprometida pela inteligência de ameaças da Amazon.

Gravidade padrão: alta

- Recurso: incluído na proteção básica da fonte de dados

Descrição completa:

Essa descoberta informa que uma chave de acesso do IAM associada à sua AWS conta foi identificada como potencialmente comprometida pela inteligência de ameaças da Amazon. A credencial comprometida foi então usada para invocar operações de API em seu ambiente. AWS A lista de chamadas de API feitas usando a credencial comprometida, junto com a contagem e os carimbos de data/hora de cada chamada, a chave de acesso envolvida e o endereço IP de origem, estão incluídos nos detalhes da descoberta.

O comprometimento de credenciais nessa descoberta é identificado pela inteligência de ameaças da Amazon. AWS monitora credenciais potencialmente comprometidas por meio de padrões de uso e gera essa descoberta quando tal credencial é observada sendo usada.

Recomendações de correção:

Se essa atividade for inesperada, suas credenciais podem estar comprometidas. Para obter mais informações, consulte Correção de problemas potencialmente comprometidos AWS credenciais.

DefenseEvasion:IAMUser/AnomalousBehavior

Uma API usada para evitar medidas defensivas foi invocada de forma anômala.

Gravidade padrão: média

- Fonte de dados: evento CloudTrail de gerenciamento

Essa descoberta informa que uma solicitação de API anômala foi observada em sua conta. Essa descoberta pode incluir uma única API ou uma série de solicitações de API relacionadas feitas na proximidade por uma única identidade de usuário. Comumente, a API observada é associada a táticas de evasão de defesa, nas quais um adversário está tentando encobrir seus rastros e evitar ser detectado. As APIs nessa categoria geralmente são operações de exclusão, desabilitação ou interrupção, como `DeleteFlowLogs`, `DisableAlarmActions` ou `StopLogging`.

Essa solicitação de API foi identificada como anômala pelo modelo de aprendizado GuardDuty de máquina (ML) de detecção de anomalias. O modelo de ML avalia todas as solicitações de API em sua conta e identifica eventos anômalos associados às técnicas usadas pelos adversários. O modelo de ML rastreia vários fatores da solicitação de API, como o usuário que fez a solicitação, o local de onde a solicitação foi feita e a API específica que foi solicitada. Os detalhes sobre quais fatores da solicitação de API são incomuns para a identidade do usuário que invocou a solicitação podem ser encontrados nos detalhes da descoberta.

Recomendações de correção:

Se essa atividade for inesperada, suas credenciais podem estar comprometidas. Para obter mais informações, consulte Correção de problemas potencialmente comprometidos AWS credenciais.

DefenseEvasion:IAMUser/BedrockLoggingDisabled

O registro em log no Amazon Bedrock foi desabilitado.

Gravidade padrão: média

- Fonte de dados: eventos CloudTrail de gerenciamento

Essa descoberta informa que o registro em log foi desabilitado para invocações do modelo do Bedrock em sua conta. Isso pode ser uma tentativa de um invasor de ocultar atividades mal-intencioandas, como exfiltração de dados ou abuso de modelos de IA. A desabilitação do registro em log remove a visibilidade dos dados enviados aos modelos e de como os modelos são usados.

Recomendações de correção:

Se essa atividade for inesperada, suas credenciais podem estar comprometidas. Para obter mais informações, consulte Correção de problemas potencialmente comprometidos AWS credenciais.

Discovery:IAMUser/AnomalousBehavior

Uma API comumente usada para descobrir recursos foi invocada de forma anômala.

Gravidade padrão: baixa

- Fonte de dados: evento CloudTrail de gerenciamento

Essa descoberta informa que uma solicitação de API anômala foi observada em sua conta. Essa descoberta pode incluir uma única API ou uma série de solicitações de API relacionadas feitas na proximidade por uma única identidade de usuário. A API observada é comumente associada ao estágio de descoberta de um ataque, quando um adversário coleta informações para determinar se seu AWS ambiente é suscetível a um ataque mais amplo. As APIs nessa categoria geralmente são operações de obtenção, descrição ou lista, como `DescribeInstances`, `GetRolePolicy` ou `ListAccessKeys`.

Essa solicitação de API foi identificada como anômala pelo modelo de aprendizado GuardDuty de máquina (ML) de detecção de anomalias. O modelo de ML avalia todas as solicitações de API em

sua conta e identifica eventos anômalos associados às técnicas usadas pelos adversários. O modelo de ML rastreia vários fatores da solicitação de API, como o usuário que fez a solicitação, o local de onde a solicitação foi feita e a API específica que foi solicitada. Os detalhes sobre quais fatores da solicitação de API são incomuns para a identidade do usuário que invocou a solicitação podem ser encontrados nos detalhes da descoberta.

Recomendações de correção:

Se essa atividade for inesperada, suas credenciais podem estar comprometidas. Para obter mais informações, consulte Correção de problemas potencialmente comprometidos AWS credenciais.

Exfiltration:IAMUser/AnomalousBehavior

Uma API comumente usada para coletar dados de um AWS o ambiente foi invocado de forma anômala.

Gravidade padrão: alta

- Fonte de dados: evento CloudTrail de gerenciamento

Essa descoberta informa que uma solicitação de API anômala foi observada em sua conta. Essa descoberta pode incluir uma única API ou uma série de solicitações de API relacionadas feitas na proximidade por uma única identidade de usuário. Comumente, a API observada é associada a táticas de exfiltração em que um adversário está tentando coletar dados de sua rede usando empacotamento e criptografia para evitar a detecção. As APIs para esse tipo de descoberta são apenas operações de gerenciamento (ambiente de gerenciamento) e geralmente estão relacionadas ao S3, aos snapshots e aos bancos de dados, como `PutBucketReplication`, `CreateSnapshot` ou `RestoreDBInstanceFromDBSnapshot`.

Essa solicitação de API foi identificada como anômala pelo modelo de aprendizado GuardDuty de máquina (ML) de detecção de anomalias. O modelo de ML avalia todas as solicitações de API em sua conta e identifica eventos anômalos associados às técnicas usadas pelos adversários. O modelo de ML rastreia vários fatores da solicitação de API, como o usuário que fez a solicitação, o local de onde a solicitação foi feita e a API específica que foi solicitada. Os detalhes sobre quais fatores da solicitação de API são incomuns para a identidade do usuário que invocou a solicitação podem ser encontrados nos detalhes da descoberta.

Recomendações de correção:

Se essa atividade for inesperada, suas credenciais podem estar comprometidas. Para obter mais informações, consulte Correção de problemas potencialmente comprometidos AWS credenciais.

Impact:IAMUser/AnomalousBehavior

Uma API comumente usada para adulterar dados ou processos em um AWS o ambiente foi invocado de forma anômala.

Gravidade padrão: alta

- Fonte de dados: evento CloudTrail de gerenciamento

Essa descoberta informa que uma solicitação de API anômala foi observada em sua conta. Essa descoberta pode incluir uma única API ou uma série de solicitações de API relacionadas feitas na proximidade por uma única identidade de usuário. Comumente, a API observada é associada a táticas de impacto em que um adversário está tentando interromper as operações e manipular, interromper ou destruir dados em sua conta. As APIs para esse tipo de descoberta geralmente são operações de exclusão, atualização ou colocação, como `DeleteSecurityGroup`, `UpdateUser` ou `PutBucketPolicy`.

Essa solicitação de API foi identificada como anômala pelo modelo de aprendizado GuardDuty de máquina (ML) de detecção de anomalias. O modelo de ML avalia todas as solicitações de API em sua conta e identifica eventos anômalos associados às técnicas usadas pelos adversários. O modelo de ML rastreia vários fatores da solicitação de API, como o usuário que fez a solicitação, o local de onde a solicitação foi feita e a API específica que foi solicitada. Os detalhes sobre quais fatores da solicitação de API são incomuns para a identidade do usuário que invocou a solicitação podem ser encontrados nos detalhes da descoberta.

Recomendações de correção:

Se essa atividade for inesperada, suas credenciais podem estar comprometidas. Para obter mais informações, consulte Correção de problemas potencialmente comprometidos AWS credenciais.

InitialAccess:IAMUser/AnomalousBehavior

Uma API comumente usada para obter acesso não autorizado a um AWS o ambiente foi invocado de forma anômala.

Gravidade padrão: média

- Fonte de dados: evento CloudTrail de gerenciamento

Essa descoberta informa que uma solicitação de API anômala foi observada em sua conta. Essa descoberta pode incluir uma única API ou uma série de solicitações de API relacionadas feitas na proximidade por uma única identidade de usuário. Comumente, a API observada é associada ao estágio inicial de acesso de um ataque, quando um adversário está tentando estabelecer acesso ao seu ambiente. As APIs nessa categoria geralmente são operações de token de obtenção ou de sessão, como `StartSession` ou `GetAuthorizationToken`.

Essa solicitação de API foi identificada como anômala pelo modelo de aprendizado GuardDuty de máquina (ML) de detecção de anomalias. O modelo de ML avalia todas as solicitações de API em sua conta e identifica eventos anômalos associados às técnicas usadas pelos adversários. O modelo de ML rastreia vários fatores da solicitação de API, como o usuário que fez a solicitação, o local de onde a solicitação foi feita e a API específica que foi solicitada. Os detalhes sobre quais fatores da solicitação de API são incomuns para a identidade do usuário que invocou a solicitação podem ser encontrados nos detalhes da descoberta.

Recomendações de correção:

Se essa atividade for inesperada, suas credenciais podem estar comprometidas. Para obter mais informações, consulte Correção de problemas potencialmente comprometidos AWS credenciais.

PenTest:IAMUser/KaliLinux

Uma API foi invocada de uma máquina Linux Kali.

Gravidade padrão: média

- Fonte de dados: evento CloudTrail de gerenciamento

Essa descoberta informa que uma máquina executando o Kali Linux está fazendo chamadas de API usando credenciais que pertencem à AWS conta listada em seu ambiente. O Kali Linux é uma ferramenta conhecida de teste de penetração usada por profissionais de segurança para identificar vulnerabilidades em instâncias do EC2 que exigem correções. Os invasores também usam essa ferramenta para encontrar pontos fracos na configuração do EC2 e obter acesso não autorizado ao seu ambiente. AWS

Recomendações de correção:

Se essa atividade for inesperada, suas credenciais podem estar comprometidas. Para obter mais informações, consulte Correção de problemas potencialmente comprometidos AWS credenciais.

PenTest:IAMUser/ParrotLinux

Uma API foi invocada a partir de uma máquina Parrot Security Linux.

Gravidade padrão: média

- Fonte de dados: evento CloudTrail de gerenciamento

Essa descoberta informa que uma máquina executando o Parrot Security Linux está fazendo chamadas de API usando credenciais que pertencem à AWS conta listada em seu ambiente. O Parrot Security Linux é uma ferramenta popular de teste de penetração que profissionais de segurança usam para identificar vulnerabilidades nas instâncias do EC2 que exigem correções. Os invasores também usam essa ferramenta para encontrar pontos fracos na configuração do EC2 e obter acesso não autorizado ao seu ambiente. AWS

Recomendações de correção:

Se essa atividade for inesperada, suas credenciais podem estar comprometidas. Para obter mais informações, consulte Correção de problemas potencialmente comprometidos AWS credenciais.

PenTest:IAMUser/PentooLinux

Uma API foi invocada a partir de uma máquina Pentoo Linux.

Gravidade padrão: média

- Fonte de dados: evento CloudTrail de gerenciamento

Essa descoberta informa que uma máquina executando o Pentoo Linux está fazendo chamadas de API usando credenciais que pertencem à AWS conta listada em seu ambiente. O Pentoo Linux é uma ferramenta conhecida de teste de penetração usada por profissionais de segurança para identificar vulnerabilidades em instâncias do EC2 que exigem correções. Os invasores também usam essa ferramenta para encontrar pontos fracos na configuração do EC2 e obter acesso não autorizado ao seu ambiente. AWS

Recomendações de correção:

Se essa atividade for inesperada, suas credenciais podem estar comprometidas. Para obter mais informações, consulte Correção de problemas potencialmente comprometidos AWS credenciais.

Persistence:IAMUser/AnomalousBehavior

Uma API comumente usada para manter o acesso não autorizado a um AWS o ambiente foi invocado de forma anômala.

Gravidade padrão: média

- Fonte de dados: evento CloudTrail de gerenciamento

Essa descoberta informa que uma solicitação de API anômala foi observada em sua conta. Essa descoberta pode incluir uma única API ou uma série de solicitações de API relacionadas feitas na proximidade por uma única identidade de usuário. Comumente, a API observada é associada a táticas de persistência em que um adversário obteve acesso ao seu ambiente e está tentando manter esse acesso. As APIs nessa categoria geralmente são operações de criação, importação ou modificação, como `CreateAccessKey`, `ImportKeyPair` ou `ModifyInstanceAttribute`.

Essa solicitação de API foi identificada como anômala pelo modelo de aprendizado GuardDuty de máquina (ML) de detecção de anomalias. O modelo de ML avalia todas as solicitações de API em sua conta e identifica eventos anômalos associados às técnicas usadas pelos adversários. O modelo de ML rastreia vários fatores da solicitação de API, como o usuário que fez a solicitação, o local de onde a solicitação foi feita e a API específica que foi solicitada. Os detalhes sobre quais fatores da solicitação de API são incomuns para a identidade do usuário que invocou a solicitação podem ser encontrados nos detalhes da descoberta.

Recomendações de correção:

Se essa atividade for inesperada, suas credenciais podem estar comprometidas. Para obter mais informações, consulte Correção de problemas potencialmente comprometidos AWS credenciais.

Policy:IAMUser/RootCredentialUsage

Foi invocada uma API usando credenciais de login do usuário raiz.

Gravidade padrão: baixa

- Fonte de dados: eventos CloudTrail de gerenciamento ou eventos CloudTrail de dados para o S3

Essa descoberta informa que as credenciais de login do usuário raiz da Conta da AWS listada em seu ambiente estão sendo usadas para fazer solicitações aos serviços da AWS . É recomendável que os usuários nunca usem as credenciais de login do usuário root para acessar os serviços. AWS Em vez disso, AWS os serviços devem ser acessados usando credenciais temporárias de privilégio mínimo de AWS Security Token Service (STS). Para situações em que o AWS STS não é compatível, é recomendável usar credenciais de usuário do IAM. Para obter mais informações, consulte Melhores práticas do IAM.

> **Note**
>
> Se a Proteção de S3 estiver habilitada para a conta, essa descoberta poderá ser gerada em resposta às tentativas de executar operações do plano de dados do S3 nos recursos do Amazon S3 usando as credenciais de login do Conta da AWS. A chamada de API usada será listada nos detalhes da descoberta. Se a Proteção do S3 não estiver habilitada, essa descoberta só poderá ser acionada pelas APIs de log de eventos. Para obter mais informações sobre a proteção de S3, consulte Proteção do S3.

Recomendações de correção:

Se essa atividade for inesperada, suas credenciais podem estar comprometidas. Para obter mais informações, consulte Correção de problemas potencialmente comprometidos AWS credenciais.

Policy:IAMUser/ShortTermRootCredentialUsage

Uma API foi invocada usando credenciais restritas de usuário-raiz.

Gravidade padrão: baixa

- Fonte de dados: eventos AWS CloudTrail de gerenciamento ou eventos AWS CloudTrail de dados para o S3

Essa descoberta informa que as credenciais de usuário restritas criadas para os listados Conta da AWS em seu ambiente estão sendo usadas para fazer solicitações para. Serviços da AWS Recomenda-se usar as credenciais de usuário-raiz somente para aquelas tarefas que exigem credenciais de usuário-raiz.

Quando possível, acesse o Serviços da AWS usando funções do IAM com privilégios mínimos com credenciais temporárias de AWS Security Token Service ()AWS STS. Para cenários em que não

AWS STS há suporte, a melhor prática é usar as credenciais de usuário do IAM. Para obter mais informações, consulte Práticas recomendadas de segurança no IAM e Práticas recomendadas para o usuário-raiz para sua Conta da AWS no Guia do usuário do IAM.

Recomendações de correção:

Se essa atividade for inesperada, suas credenciais podem estar comprometidas. Para obter mais informações, consulte Correção de problemas potencialmente comprometidos AWS credenciais.

PrivilegeEscalation:IAMUser/AnomalousBehavior

Uma API comumente usada para obter permissões de alto nível para um AWS o ambiente foi invocado de forma anômala.

Gravidade padrão: média

- Fonte de dados: eventos CloudTrail de gerenciamento

Essa descoberta informa que uma solicitação de API anômala foi observada em sua conta. Essa descoberta pode incluir uma única API ou uma série de solicitações de API relacionadas feitas na proximidade por uma única identidade de usuário. Comumente, a API observada é associada a táticas de escalonamento de privilégios em que um adversário está tentando obter permissões de nível superior para um ambiente. As APIs nessa categoria geralmente envolvem operações que alteram políticas, perfis e usuários do IAM, como `AssociateIamInstanceProfile`, `AddUserToGroup` ou `PutUserPolicy`.

Essa solicitação de API foi identificada como anômala pelo modelo de aprendizado GuardDuty de máquina (ML) de detecção de anomalias. O modelo de ML avalia todas as solicitações de API em sua conta e identifica eventos anômalos associados às técnicas usadas pelos adversários. O modelo de ML rastreia vários fatores da solicitação de API, como o usuário que fez a solicitação, o local de onde a solicitação foi feita e a API específica que foi solicitada. Os detalhes sobre quais fatores da solicitação de API são incomuns para a identidade do usuário que invocou a solicitação podem ser encontrados nos detalhes da descoberta.

Recomendações de correção:

Se essa atividade for inesperada, suas credenciais podem estar comprometidas. Para obter mais informações, consulte Correção de problemas potencialmente comprometidos AWS credenciais.

Recon:IAMUser/MaliciousIPCaller

Uma API foi invocada a partir de um endereço IP mal-intencionado conhecido.

Gravidade padrão: média

- Fonte de dados: eventos CloudTrail de gerenciamento

Essa descoberta informa que uma operação de API que pode listar ou descrever recursos em uma conta no seu ambiente da AWS foi invocada a partir de um endereço IP incluído em uma lista de ameaças. Um invasor pode usar credenciais roubadas para realizar esse tipo de reconhecimento de seus AWS recursos a fim de encontrar credenciais mais valiosas ou determinar as capacidades das credenciais que ele já possui.

Recomendações de correção:

Se essa atividade for inesperada, suas credenciais podem estar comprometidas. Para obter mais informações, consulte Correção de problemas potencialmente comprometidos AWS credenciais.

Recon:IAMUser/MaliciousIPCaller.Custom

Uma API foi invocada a partir de um endereço IP mal-intencionado conhecido.

Gravidade padrão: média

- Fonte de dados: eventos CloudTrail de gerenciamento

Essa descoberta informa que uma operação de API que pode listar ou descrever recursos em uma conta dentro do seu ambiente da AWS foi invocada a partir de um endereço IP incluído em uma lista de ameaças personalizada. A lista de ameaças usada será indicada nos detalhes da descoberta. Um invasor pode usar credenciais roubadas para realizar esse tipo de reconhecimento de seus AWS recursos a fim de encontrar credenciais mais valiosas ou determinar as capacidades das credenciais que ele já possui.

Recomendações de correção:

Se essa atividade for inesperada, suas credenciais podem estar comprometidas. Para obter mais informações, consulte Correção de problemas potencialmente comprometidos AWS credenciais.

Recon:IAMUser/TorIPCaller

Uma API foi invocada a partir de um endereço IP do nó de saída do Tor.

Gravidade padrão: média

- Fonte de dados: eventos CloudTrail de gerenciamento

Essa descoberta informa que uma operação de API que pode listar ou descrever recursos em uma conta no seu ambiente da AWS foi invocada de um endereço IP de nó de saída Tor. Tor é um software para permitir a comunicação anônima. Ele criptografa e aleatoriamente envia comunicações por meio de relés entre uma série de nós de rede. O último nó do Tor é chamado de nó de saída. Um atacante usaria o Tor para mascarar sua verdadeira identidade.

Recomendações de correção:

Se essa atividade for inesperada, suas credenciais podem estar comprometidas. Para obter mais informações, consulte Correção de problemas potencialmente comprometidos AWS credenciais.

Stealth:IAMUser/CloudTrailLoggingDisabled

AWS CloudTrail o registro foi desativado.

Gravidade padrão: baixa

- Fonte de dados: eventos CloudTrail de gerenciamento

Essa descoberta informa que uma CloudTrail trilha em seu AWS ambiente foi desativada. Isso pode ser uma tentativa de um invasor de desabilitar a gravação de logs para não deixar rastros, eliminando quaisquer evidências da atividade dele ao obter acesso aos seus recursos da AWS para fins mal-intencionados. Essa descoberta pode ser acionada por uma exclusão ou atualização bem-sucedida de uma trilha. Essa descoberta também pode ser acionada por uma exclusão bem-sucedida de um bucket do S3 que armazena os registros de uma trilha associada a. GuardDuty

Recomendações de correção:

Se essa atividade for inesperada, suas credenciais podem estar comprometidas. Para obter mais informações, consulte Correção de problemas potencialmente comprometidos AWS credenciais.

Stealth:IAMUser/PasswordPolicyChange

A política de senha da conta foi enfraquecida.

Gravidade padrão: baixa*

> **Note**
>
> A gravidade dessa descoberta pode ser baixa, média ou alta, dependendo da gravidade das alterações feitas na política de senhas.

- Fonte de dados: eventos CloudTrail de gerenciamento

A política de senha da AWS conta foi enfraquecida na conta listada em seu AWS ambiente. Por exemplo, ela foi excluída ou atualizada para exigir menos caracteres, não requer símbolos nem números ou precisou prolongar o período de validade da senha. Essa descoberta também pode ser desencadeada por uma tentativa de atualizar ou excluir a política de senha AWS da sua conta. A política de senha da AWS conta define as regras que regem quais tipos de senhas podem ser definidos para seus usuários do IAM. Uma política de senha mais fraca permite a criação de senhas fáceis de lembrar e possivelmente mais fáceis de adivinhar, criando um risco à segurança.

Recomendações de correção:

Se essa atividade for inesperada, suas credenciais podem estar comprometidas. Para obter mais informações, consulte Correção de problemas potencialmente comprometidos AWS credenciais.

UnauthorizedAccess:IAMUser/ConsoleLoginSuccess.B

Foram observados vários logins de console bem-sucedidos em todo o mundo.

Gravidade padrão: média

- Fonte de dados: eventos CloudTrail de gerenciamento

Essa descoberta informa que foram observados vários logins bem-sucedidos no console para o mesmo usuário do IAM por volta do mesmo horário em vários locais geográficos. Esses padrões de localização de acesso anômalos e arriscados indicam um possível acesso não autorizado aos seus recursos. AWS

Recomendações de correção:

Se essa atividade for inesperada, suas credenciais podem estar comprometidas. Para obter mais informações, consulte Correção de problemas potencialmente comprometidos AWS credenciais.

UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.InsideAWS

As credenciais que foram criadas exclusivamente para uma instância do EC2 por meio de uma função de inicialização de instância estão sendo usadas de outra conta dentro AWS.

Gravidade padrão: alta*

> **Note**
>
> A gravidade padrão desta descoberta é baixa. No entanto, se a API foi invocada por uma conta afiliada ao seu AWS ambiente, a gravidade é Média.

- Fonte de dados: eventos CloudTrail de gerenciamento ou eventos CloudTrail de dados para o S3

Essa descoberta informa quando suas credenciais de instância do Amazon EC2 são usadas para invocar APIs de um endereço IP ou de um endpoint da Amazon VPC, que pertence a uma conta AWS diferente daquela em que a instância associada do Amazon EC2 está sendo executada. A detecção de endpoints de VPC só está disponível para serviços que oferecem suporte a eventos de atividade de rede para endpoints da VPC. Para obter informações sobre serviços que oferecem suporte a eventos de atividade de rede para endpoint da VPC, consulte Registro de eventos de atividade de rede no Guia do usuário do AWS CloudTrail .

AWS não recomenda redistribuir credenciais temporárias fora da entidade que as criou (por exemplo, AWS aplicativos, Amazon EC2 ou). AWS Lambda No entanto, usuários autorizados podem exportar credenciais de suas instâncias do Amazon EC2 para fazer chamadas legítimas de API. Se o campo `remoteAccountDetails.Affiliated` for `True`, a API foi invocada de uma conta associada à mesma conta de administrador. Para descartar um possível ataque e verificar a legitimidade da atividade, entre em contato com o Conta da AWS proprietário ou o diretor do IAM a quem essas credenciais foram atribuídas.

> **Note**
>
> Se GuardDuty observar a atividade contínua de uma conta remota, seu modelo de aprendizado de máquina (ML) identificará isso como um comportamento esperado. Portanto, GuardDuty deixará de gerar essa descoberta para atividades dessa conta remota. GuardDuty continuará gerando descobertas sobre novos comportamentos de outras contas remotas e reavaliará as contas remotas aprendidas à medida que o comportamento muda com o tempo.

Recomendações de correção:

Essa descoberta é gerada quando as solicitações de AWS API são feitas internamente AWS por meio de uma instância do Amazon EC2 fora da sua Conta da AWS, usando as credenciais de sessão da sua instância do Amazon EC2. Pode ser comum, como na arquitetura Transit Gateway em uma configuração de hub and spoke, rotear o tráfego por meio de uma única VPC de saída de hub com endpoints de serviço. AWS Se esse comportamento for esperado, então GuardDuty recomenda que você use Regras de supressão e crie uma regra com critérios de dois filtros. O primeiro critério é o tipo de descoberta, que, nesse caso, é UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.InsideAWS. O segundo critério de filtro é o ID da conta remota dos detalhes da conta remota.

Em resposta a essa descoberta, é possível usar o seguinte fluxo de trabalho para determinar um curso de ação:

1. Identifique a conta remota envolvida no campo `service.action.awsApiCallAction.remoteAccountDetails.accountId`.
2. Determine se essa conta é afiliada ao seu GuardDuty ambiente a partir do `service.action.awsApiCallAction.remoteAccountDetails.affiliated` campo.
3. Se a conta for afiliada, entre em contato com o proprietário da conta remota e com o proprietário das credenciais da instância Amazon EC2 para investigar.

   Se a conta não for afiliada, a primeira etapa é avaliar se essa conta está associada à sua organização, mas não faz parte da configuração do seu ambiente GuardDuty de várias contas ou se ainda não GuardDuty foi ativada nessa conta. Caso contrário, entre em contato com o proprietário das credenciais de instância do Amazon EC2 para determinar se há um caso de uso para uma conta remota usar essas credenciais.

4. Se o proprietário das credenciais não reconhecer a conta remota, as credenciais podem ter sido comprometidas por um agente de ameaça operando na AWS. Siga as etapas recomendadas em Como corrigir uma instância do Amazon EC2 potencialmente comprometida, para proteger seu ambiente.

   Além disso, você pode enviar uma denúncia de abuso à equipe de AWS Confiança e Segurança para iniciar uma investigação sobre a conta remota. Ao enviar seu relatório para o AWS Trust and Safety, inclua todos os detalhes do JSON da descoberta.

UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS

As credenciais criadas exclusivamente para uma instância do EC2 pela função de execução de uma instância estão sendo usadas por um endereço IP externo.

Gravidade padrão: alta

- Fonte de dados: eventos CloudTrail de gerenciamento ou eventos CloudTrail de dados para o S3

Essa descoberta informa que um host externo AWS tentou executar operações de AWS API usando AWS credenciais temporárias que foram criadas em uma instância do EC2 em seu ambiente. AWS A instância EC2 listada pode estar comprometida e as credenciais temporárias dessa instância podem ter sido transferidas para um host remoto externo. AWS AWS não recomenda redistribuir credenciais temporárias fora da entidade que as criou (por exemplo, AWS aplicativos, EC2 ou Lambda). No entanto, os usuários autorizados podem exportar credenciais das respectivas instâncias do EC2 para fazer chamadas de API legítimas. Para descartar um possível ataque e verificar a legitimidade da atividade, valide se o uso de credenciais de instância do IP remoto na descoberta é esperado.

> **Note**
>
> Se GuardDuty observar a atividade contínua de um host remoto, seu modelo de aprendizado de máquina (ML) identificará isso como um comportamento esperado. Portanto, GuardDuty deixará de gerar essa descoberta para atividades desse host remoto. GuardDuty continuará gerando descobertas sobre novos comportamentos de outros hosts remotos e reavaliará os hosts remotos aprendidos à medida que o comportamento muda com o tempo.

Recomendações de correção:

Essa descoberta é gerada quando a rede é configurada para rotear o tráfego da Internet de modo que ele saia de um gateway on-premises e não de um gateway da Internet (IGW) da VPC. Configurações comuns, como usar AWS Outposts, ou conexões de VPN da VPC podem resultar em tráfego roteado dessa maneira. Se esse comportamento for esperado, é recomendável usar regras de supressão e criar uma regra que consista em dois critérios de filtro. O primeiro critério é tipo de descoberta, que deve ser `UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS`. O segundo critério de filtro é o endereço IPv4 do chamador de API com o endereço IP ou intervalo CIDR do seu gateway da Internet on-premises. Para saber mais sobre a criação de regras de supressão, consulte Regras de supressão em GuardDuty.

> **Note**
>
> Se GuardDuty observar a atividade contínua de uma fonte externa, seu modelo de aprendizado de máquina identificará isso como comportamento esperado e deixará de gerar essa descoberta para atividades dessa fonte. GuardDuty continuará gerando descobertas sobre novos comportamentos a partir de outras fontes e reavaliará as fontes aprendidas à medida que o comportamento muda com o tempo.

Se essa atividade for inesperada, suas credenciais podem estar comprometidas. Consulte Correção de problemas potencialmente comprometidos AWS credenciais.

UnauthorizedAccess:IAMUser/MaliciousIPCaller

Uma API foi invocada a partir de um endereço IP mal-intencionado conhecido.

Gravidade padrão: média

- Fonte de dados: eventos CloudTrail de gerenciamento

Essa descoberta informa que uma operação de API (por exemplo, uma tentativa de iniciar uma instância do EC2, criar um novo usuário do IAM ou modificar seus privilégios da AWS) foi invocada a partir de um endereço IP mal-intencionado conhecido. Isso pode indicar acesso não autorizado aos AWS recursos em seu ambiente.

Recomendações de correção:

Se essa atividade for inesperada, suas credenciais podem estar comprometidas. Para obter mais informações, consulte Correção de problemas potencialmente comprometidos AWS credenciais.

UnauthorizedAccess:IAMUser/MaliciousIPCaller.Custom

Uma API foi invocada a partir de um endereço IP em uma lista de ameaças personalizada.

Gravidade padrão: média

- Fonte de dados: eventos CloudTrail de gerenciamento

Essa descoberta informa que uma operação de API (por exemplo, uma tentativa de iniciar uma instância do EC2, criar um novo usuário do IAM ou modificar AWS privilégios) foi invocada a partir de um endereço IP incluído em uma lista de ameaças que você enviou. Em GuardDuty, uma lista de ameaças consiste em endereços IP maliciosos conhecidos. Isso pode indicar acesso não autorizado aos AWS recursos em seu ambiente.

Recomendações de correção:

Se essa atividade for inesperada, suas credenciais podem estar comprometidas. Para obter mais informações, consulte Correção de problemas potencialmente comprometidos AWS credenciais.

UnauthorizedAccess:IAMUser/ResourceCredentialExfiltration.InsideAWS

Credenciais que foram criadas exclusivamente para um AWS Tarefa do Amazon ECS ou AWS A função Lambda está sendo usada em outra conta dentro AWS

Gravidade padrão: alta*

> **Note**
>
> A gravidade padrão desta descoberta é baixa. No entanto, se a API foi invocada por uma conta afiliada ao seu AWS ambiente, a gravidade é Média.

- Fonte de dados: eventos CloudTrail de gerenciamento ou eventos CloudTrail de dados para o S3

Essa descoberta informa quando suas credenciais de tarefa do AWS Amazon ECS ou credenciais da função AWS Lambda são usadas para invocar APIs de um endereço IP ou de um endpoint do Amazon VPC, que pertence a uma AWS conta diferente daquela em que o recurso associado está sendo executado. A detecção de endpoints de VPC só está disponível para serviços que oferecem suporte a eventos de atividade de rede para endpoints da VPC. Para obter informações sobre serviços que oferecem suporte a eventos de atividade de rede para endpoint da VPC, consulte Registro de eventos de atividade de rede no Guia do usuário do AWS CloudTrail .

AWS não recomenda redistribuir credenciais temporárias fora da entidade que as criou (por exemplo, AWS aplicativos, Amazon EC2 ou Amazon Elastic Container Service). No entanto, usuários autorizados podem exportar credenciais de seus recursos para fazer chamadas legítimas de API. Se o `remoteAccountDetails.affiliated` campo `True` for, significa que a API foi invocada de uma conta associada à mesma conta de administrador. Para descartar um possível ataque e verificar a legitimidade da atividade, entre em contato com o Conta da AWS proprietário ou o diretor do IAM a quem essas credenciais foram atribuídas.

> **Note**
>
> Se GuardDuty observar a atividade contínua de uma conta remota, seu modelo de aprendizado de máquina (ML) identificará isso como um comportamento esperado. Portanto, GuardDuty deixará de gerar essa descoberta para atividades dessa conta remota. GuardDuty continuará gerando descobertas sobre novos comportamentos de outras contas remotas e reavaliará as contas remotas aprendidas à medida que o comportamento muda com o tempo.

> **Note**
>
> Para tarefas do Amazon ECS, as credenciais são associadas à função da tarefa e a detecção se aplica independentemente da configuração da VPC.

Recomendações de correção:

Essa descoberta é gerada quando as solicitações de AWS API são feitas internamente AWS por meio de um recurso externo ao seu Conta da AWS, usando suas credenciais de tarefa do AWS Amazon ECS ou credenciais da função AWS Lambda. Pode ser comum, como na arquitetura Transit Gateway em uma configuração de hub and spoke, rotear o tráfego por meio de uma única

VPC de saída de hub com endpoints de serviço. AWS Se esse for o comportamento esperado, recomendamos que você use Regras de supressão com critérios de filtro o tipo de localização, que deveria serUnauthorizedAccess:IAMUser/ResourceCredentialExfiltration.InsideAWS.

Em resposta a essa descoberta, é possível usar o seguinte fluxo de trabalho para determinar um curso de ação:

1. Identifique a conta remota envolvida no campo `service.action.awsApiCallAction.remoteAccountDetails.accountId`.
2. Determine se essa conta é afiliada ao seu GuardDuty ambiente a partir do `service.action.awsApiCallAction.remoteAccountDetails.affiliated` campo.
3. Se a conta for afiliada, entre em contato com o proprietário da conta remota e com o proprietário das credenciais do recurso para investigar.

   Se a conta não for afiliada, a primeira etapa é avaliar se essa conta está associada à sua organização, mas não faz parte da configuração do seu ambiente GuardDuty de várias contas ou se ainda não GuardDuty foi ativada nessa conta. Em seguida, entre em contato com o proprietário das credenciais do recurso para determinar se há um caso de uso para uma conta remota usar essas credenciais.
4. Se o proprietário das credenciais não reconhecer a conta remota, as credenciais podem ter sido comprometidas por um agente de ameaça operando na AWS. Siga as etapas recomendadas em Como corrigir um cluster do ECS possivelmente comprometido, para proteger seu ambiente.

   Além disso, você pode enviar uma denúncia de abuso à equipe de AWS Confiança e Segurança para iniciar uma investigação sobre a conta remota. Ao enviar seu relatório para o AWS Trust and Safety, inclua todos os detalhes do JSON da descoberta.

UnauthorizedAccess:IAMUser/ResourceCredentialExfiltration.OutsideAWS

Credenciais que foram criadas exclusivamente para um AWS recursos, (uma função Lambda ou tarefa do Amazon ECS), estão sendo usados a partir de um endereço IP fora do AWS.

Gravidade padrão: alta

- Fonte de dados: eventos CloudTrail de gerenciamento ou eventos CloudTrail de dados para o S3

Essa descoberta informa que um host externo AWS tentou executar operações de AWS API usando AWS credenciais temporárias que foram criadas em um AWS recurso (uma função Lambda ou uma tarefa do Amazon ECS) em seu ambiente. AWS O recurso listado pode estar comprometido e as credenciais temporárias desse recurso podem ter sido exfiltradas para um host remoto externo. AWS

AWS não recomenda redistribuir credenciais temporárias fora da entidade que as criou (por exemplo, aplicativos AWS como Amazon Elastic Compute Cloud (Amazon EC2), Amazon Elastic Container Service ou). AWS Lambda No entanto, usuários autorizados podem exportar credenciais de seus recursos para fazer chamadas legítimas de API. Para descartar um possível ataque e verificar a legitimidade da atividade, valide se o uso de credenciais de recursos do IP remoto na descoberta é esperado.

> **Note**
>
> Se GuardDuty observar a atividade contínua de um host remoto, seu modelo de aprendizado de máquina (ML) identificará isso como um comportamento esperado. Portanto, GuardDuty deixará de gerar essa descoberta para atividades desse host remoto. GuardDuty continuará gerando descobertas sobre novos comportamentos de outros hosts remotos e reavaliará os hosts remotos aprendidos à medida que o comportamento muda com o tempo.

Recomendações de correção:

Essa descoberta é gerada quando a rede é configurada para rotear o tráfego da internet de modo que ele saia de um gateway on-premises e não de um gateway da internet (IGW) da VPC. Configurações comuns, como usar AWS Outposts, ou conexões de VPN da VPC podem fazer com que o tráfego seja roteado dessa maneira. Se esse for o comportamento esperado, então GuardDuty recomenda usar Regras de supressão para criar uma regra com critérios de dois filtros. O primeiro critério é tipo de descoberta, que deve ser `UnauthorizedAccess:IAMUser/ResourceCredentialExfiltration.OutsideAWS`. O segundo critério de filtro é o endereço IPv4 do chamador de API com o endereço IP ou intervalo CIDR do gateway da internet on-premises.

Se essa atividade for inesperada, suas credenciais podem ter sido comprometidas. Para obter informações sobre as etapas para corrigir esse tipo de descobertaCorreção de problemas potencialmente comprometidos AWS credenciais, consulte ouComo corrigir um cluster do ECS possivelmente comprometido.

UnauthorizedAccess:IAMUser/TorIPCaller

Uma API foi invocada a partir de um endereço IP do nó de saída do Tor.

Gravidade padrão: média

- Fonte de dados: eventos CloudTrail de gerenciamento

Essa descoberta informa que uma operação da API (por exemplo, uma tentativa de iniciar uma instância do EC2, criar um novo usuário do IAM ou modificar seus privilégios da AWS) foi invocada a partir de um endereço IP de nó de saída do Tor. Tor é um software para permitir a comunicação anônima. Ele criptografa e aleatoriamente envia comunicações por meio de relés entre uma série de nós de rede. O último nó do Tor é chamado de nó de saída. Isso pode indicar um acesso não autorizado aos seus recursos da AWS com a intenção de ocultar a verdadeira identidade do invasor.

Recomendações de correção:

Se essa atividade for inesperada, suas credenciais podem estar comprometidas. Para obter mais informações, consulte Correção de problemas potencialmente comprometidos AWS credenciais.

GuardDuty tipos de localização de sequências de ataque

GuardDuty detecta uma sequência de ataque quando uma sequência específica de várias ações se alinha a uma atividade potencialmente suspeita. Uma sequência de ataque inclui sinais como atividades e GuardDuty descobertas da API. Quando GuardDuty observa um grupo de sinais em uma sequência específica que indica uma ameaça à segurança em andamento, contínua ou recente, GuardDuty gera uma descoberta da sequência de ataque. GuardDuty considera as atividades individuais da API weak signals porque elas não se apresentam como uma ameaça em potencial.

As detecções da sequência de ataque se concentram no possível comprometimento de dados do Amazon S3 (que podem fazer parte de um ataque mais amplo de ransomware), AWS credenciais comprometidas, clusters do Amazon EKS comprometidos, clusters do Amazon ECS comprometidos e grupos de instâncias do Amazon EC2 comprometidos. As seguintes seções fornecem detalhes sobre cada uma das sequências de ataque.

Tópicos

- AttackSequence:EKS/CompromisedCluster
- AttackSequence:ECS/CompromisedCluster

- AttackSequence:EC2/CompromisedInstanceGroup
- AttackSequence:IAM/CompromisedCredentials
- AttackSequence:S3/CompromisedData

AttackSequence:EKS/CompromisedCluster

Uma sequência de ações suspeitas executadas por um cluster potencialmente comprometido do Amazon EKS.

- Gravidade padrão: crítica
- Fontes de dados:
  - Eventos de log de auditoria do EKS
  - Monitoramento de Runtime para Amazon EKS
  - Detecção de malware no Amazon EKS para Amazon EC2
  - AWS CloudTrail eventos de dados para S3
  - AWS CloudTrail eventos de gerenciamento
  - Logs de fluxo da VPC
  - Logs de consultas de DNS do Route53 Resolver

Essa descoberta informa que GuardDuty detectou uma sequência de ações suspeitas que indica um cluster Amazon EKS potencialmente comprometido em seu ambiente. Vários comportamentos de ataque suspeitos e anômalos, como processos maliciosos ou conexão com endpoints maliciosos, foram observados no mesmo cluster do Amazon EKS.

GuardDuty usa seus algoritmos de correlação proprietários para observar e identificar a sequência de ações realizadas usando a credencial IAM. GuardDuty avalia as descobertas em planos de proteção e outras fontes de sinal para identificar padrões de ataque comuns e emergentes. GuardDuty usa vários fatores para revelar ameaças, como reputação de IP, sequências de API, configuração do usuário e recursos potencialmente afetados.

Ações de remediação: se esse comportamento for inesperado em seu ambiente, seu cluster do Amazon EKS pode estar comprometido. Para obter uma orientação abrangente sobre remediação, consulte Como corrigir as descobertas da Proteção do EKS e Como corrigir as descobertas do Monitoramento de runtime.

Além disso, como AWS as credenciais podem ter sido comprometidas por meio do cluster EKS, consulte. Correção de problemas potencialmente comprometidos AWS credenciais Para ver as etapas para remediar outros recursos que possam ter sido potencialmente afetados, consulte Corrigindo descobertas de GuardDuty segurança detectadas.

AttackSequence:ECS/CompromisedCluster

Uma sequência de ações suspeitas executadas por um cluster Amazon ECS potencialmente comprometido.

- Gravidade padrão: crítica
- Fontes de dados:
  - Monitoramento de tempo de execução para Amazon ECS Fargate
  - Monitoramento de tempo de execução para instâncias do EC2 no Amazon ECS
  - GuardDuty Proteção contra malware para Amazon EC2

Essa descoberta informa que GuardDuty detectou uma sequência de sinais suspeitos indicando um cluster Amazon ECS potencialmente comprometido em seu ambiente. Esses sinais podem incluir processos maliciosos, comunicações com terminais maliciosos ou comportamentos de mineração de criptomoedas.

GuardDuty usa algoritmos de correlação proprietários e vários fatores de detecção para identificar sequências de ações suspeitas nos clusters do Amazon ECS. Por meio da análise de planos de proteção e de várias fontes de sinal, GuardDuty identifica padrões de ataque comuns e emergentes, fornecendo uma detecção de alta confiança de possíveis comprometimentos.

Ações de remediação: se esse comportamento for inesperado em seu ambiente, seu cluster do Amazon ECS poderá estar comprometido. Para recomendações de contenção de ameaças, consulteComo corrigir um cluster do ECS possivelmente comprometido. Observe que o comprometimento pode se estender a uma ou mais tarefas do ECS ou cargas de trabalho de contêiner, que poderiam ter sido usadas para criar ou modificar AWS recursos. Para obter orientações abrangentes de remediação que abrangem os recursos potencialmente afetados, consulte. Corrigindo descobertas de GuardDuty segurança detectadas

AttackSequence:EC2/CompromisedInstanceGroup

Uma sequência de ações suspeitas indicando instâncias do Amazon EC2 potencialmente comprometidas.

- Gravidade padrão: crítica
- Fontes de dados:
  - Monitoramento de tempo de execução para o Amazon EC2
  - Detecção de malware para o Amazon EC2
  - Logs de fluxo da VPC
  - Logs de consultas de DNS do Route53 Resolver

Essa descoberta indica que GuardDuty detectou uma sequência de ações suspeitas, sugerindo um possível comprometimento em um grupo de instâncias do Amazon EC2 em seu ambiente. Os grupos de instâncias normalmente representam aplicativos gerenciados por meio de infraestrutura como código, compartilhando configurações semelhantes, como Auto-scaling grupo, função de perfil de instância do IAM, AWS CloudFormation pilha, modelo de lançamento do Amazon EC2, AMI ou ID de VPC. GuardDuty observou vários comportamentos suspeitos em uma ou mais instâncias, incluindo:

- Processos maliciosos
- Arquivos maliciosos
- Conexões de rede suspeitas
- Atividades de mineração de criptomoedas
- Uso suspeito de credenciais de instância do Amazon EC2

Método de detecção: GuardDuty emprega algoritmos de correlação proprietários para identificar sequências de ação suspeitas nas instâncias do Amazon EC2. Ao avaliar as descobertas em planos de proteção e várias fontes de sinal, GuardDuty identifica padrões de ataque usando vários fatores, como reputação de IP e domínio e processos suspeitos em execução.

Ações de remediação: se esse comportamento for inesperado em seu ambiente, suas instâncias do Amazon EC2 poderão ser comprometidas. O compromisso pode envolver:

- Vários processos

- Credenciais de instância que podem ter sido usadas para modificar instâncias do Amazon EC2 ou outros recursos AWS

Para recomendações de contenção de ameaças, consulteComo corrigir uma instância do Amazon EC2 potencialmente comprometida. Observe que o comprometimento pode se estender a uma ou mais instâncias do Amazon EC2 e envolver processos comprometidos ou credenciais de instância que poderiam ter sido usadas para criar ou modificar instâncias do Amazon EC2 ou outros recursos. AWS Para obter orientações abrangentes de remediação que abrangem os recursos potencialmente afetados, consulte. Corrigindo descobertas de GuardDuty segurança detectadas

AttackSequence:IAM/CompromisedCredentials

Uma sequência de solicitações de API que foram invocadas usando o uso potencialmente comprometido AWS credenciais.

- Gravidade padrão: crítica
- Fonte de dados: AWS CloudTrail eventos de gerenciamento

Essa descoberta informa que GuardDuty detectou uma sequência de ações suspeitas feitas com o uso de AWS credenciais que afetam um ou mais recursos em seu ambiente. Vários comportamentos de ataque suspeitos e anômalos foram observados pelas mesmas credenciais, resultando em maior confiança de que as credenciais estão sendo mal utilizadas.

GuardDuty usa seus algoritmos de correlação proprietários para observar e identificar a sequência de ações realizadas usando a credencial IAM. GuardDuty avalia as descobertas em planos de proteção e outras fontes de sinal para identificar padrões de ataque comuns e emergentes. GuardDuty usa vários fatores para revelar ameaças, como reputação de IP, sequências de API, configuração do usuário e recursos potencialmente afetados.

Quando você ativaProteção da IA, também GuardDuty pode incluir Tipos de descoberta de proteção de IA entre os sinais que ele correlaciona para essa sequência de ataque. Essas descobertas estão associadas a uma identidade do IAM. Como resultado, GuardDuty pode apresentá-los como sinais nessa sequência de ataque e correlacioná-los com outras ações suspeitas tomadas com as mesmas credenciais potencialmente comprometidas. Por exemplo, GuardDuty pode correlacionar outros sinais com uma invocação anômala do modelo Amazon Bedrock ou Amazon SageMaker AI feita com essas credenciais e incluí-la nessa sequência de ataque. Por si só, as descobertas da AI Protection não geram uma sequência de ataque. Para obter mais informações, consulte Proteção da IA.

Ações de remediação: se esse comportamento for inesperado em seu ambiente, suas AWS credenciais podem ter sido comprometidas. Para obter as etapas de correção, consulte Correção de problemas potencialmente comprometidos AWS credenciais. As credenciais comprometidas podem ter sido usadas para criar ou modificar recursos adicionais, como buckets do Amazon S3, funções AWS Lambda ou instâncias do Amazon EC2, no seu ambiente. Para ver as etapas para remediar outros recursos que possam ter sido potencialmente afetados, consulte Corrigindo descobertas de GuardDuty segurança detectadas.

AttackSequence:S3/CompromisedData

Uma sequência de solicitações de API foi invocada em uma possível tentativa de exfiltrar ou destruir dados no Amazon S3.

- Gravidade padrão: crítica
- Fontes de dados: AWS CloudTrail eventos de dados para S3 e AWS CloudTrail eventos de gerenciamento

Essa descoberta informa que GuardDuty detectou uma sequência de ações suspeitas indicativas de comprometimento de dados em um ou mais buckets do Amazon Simple Storage Service (Amazon S3), usando credenciais potencialmente comprometidas. AWS Vários comportamentos de ataque suspeitos e anômalos (solicitações de API) foram observados, resultando em maior confiança de que as credenciais estão sendo mal utilizadas.

GuardDuty usa seus algoritmos de correlação para observar e identificar a sequência de ações realizadas usando a credencial IAM. GuardDuty em seguida, avalia as descobertas em planos de proteção e outras fontes de sinal para identificar padrões de ataque comuns e emergentes. GuardDuty usa vários fatores para revelar ameaças, como reputação de IP, sequências de API, configuração do usuário e recursos potencialmente afetados.

Ações de remediação: se essa atividade for inesperada em seu ambiente, suas AWS credenciais ou dados do Amazon S3 podem ter sido potencialmente exfiltrados ou destruídos. Para obter as etapas de correção, consulte Correção de problemas potencialmente comprometidos AWS credenciais e Como corrigir um bucket do S3 possivelmente comprometido.

Tipos de localização de regras de detecção personalizadas

Esta página lista os tipos de descoberta GuardDuty gerados a partir das Regras de Detecção Personalizadas, agrupados por fonte de dados. Cada tipo de descoberta agrega um ou mais sinais

em uma única descoberta. Para obter mais informações sobre como ativar as Regras de Detecção Personalizadas, consulteRegras de detecção personalizadas em GuardDuty.

> **Note**
>
> As regras individuais estão disponíveis somente para oferecer suporte ao AWS serviço ou recurso que elas visam. Regiões da AWS Por exemplo, regras que têm como alvo AWS Organizations ou Amazon Simple Email Service estão disponíveis somente nas regiões em que esses serviços operam. Da mesma forma, as regras que têm como alvo URLs de funções do Lambda ou instâncias de notebooks de SageMaker IA estão disponíveis somente nas regiões em que esses recursos são compatíveis.

Tópicos

- Regras de detecção personalizadas para AWS CloudTrail eventos de gerenciamento
- Regras de detecção personalizadas para monitoramento de tempo de execução

Regras de detecção personalizadas para AWS CloudTrail eventos de gerenciamento

Os seguintes tipos de descoberta são gerados a partir de sinais AWS CloudTrail de eventos de gerenciamento, organizados pela MITRE ATT&CK® tactic.

Acesso credencial

Essas regras tentam detectar operações que recuperam ou redefinem credenciais, como recuperar uma senha de instância do Amazon EC2 ou redefinir uma senha de administrador do Amazon RDS.

Tipo de descoberta	Nome da regra	Gravidade
CredentialAccess:EC2/UnsecuredCredentials	EC2PasswordDataRetrieved	MÉDIO
CredentialAccess:RDS/ModifyAuthenticationProcess	RDSMasterPasswordReset	HIGH (ALTO)

Deficiência de defesa

Essas regras tentam detectar alterações que desabilitam ou enfraquecem os controles de segurança, como excluir registros de fluxo de VPC, desabilitar uma política da organização ou remover uma conta de uma organização.

Tipo de descoberta	Nome da regra	Gravidade
DefenseImpairment:EC2/DisableOrModifyTools	EC2TerminationProtectionEnabled	BAIXO
	VPCFlowLogsDeleted	HIGH (ALTO)
DefenseImpairment:Organizations/ModifyCloudResourceHierarchy	OrganizationLeaveAttempt	HIGH (ALTO)
DefenseImpairment:Organizations/DisableOrModifyTools	OrganizationPolicyDisabled	HIGH (ALTO)
DefenseImpairment:RDS/ModifyAuthenticationProcess	RDSIAMAuthDisabled	MÉDIO
DefenseImpairment:Route53Resolver/DisableOrModifyTools	DNSQueryLogsDeleted	MÉDIO
DefenseImpairment:S3/DisableOrModifyTools	S3CustomerProvidedKeysEnabled	HIGH (ALTO)

Execução

Essas regras tentam detectar alterações que executam código em um recurso, como modificar a configuração do ciclo de vida de um notebook com SageMaker IA.

Tipo de descoberta	Nome da regra	Gravidade
Execution:SageMaker/CommandAndScriptingInterpreter	SageMakerLifecycleConfigModified	MÉDIO

Exfiltration

Essas regras tentam detectar alterações que compartilham recursos fora da sua conta, como tornar um AMI, um snapshot do Amazon EBS ou um snapshot do Amazon RDS acessível a outras contas.

Tipo de descoberta	Nome da regra	Gravidade
Exfiltration:EC2/TransferDataToCloudAccount	AMIExternalAccess	HIGH (ALTO)
	EBSSnapshotExternalAccess	HIGH (ALTO)
Exfiltration:RDS/TransferDataToCloudAccount	RDSSnapshotPubliclyShared	HIGH (ALTO)
Exfiltration:S3/TransferDataToCloudAccount	S3BucketPolicyExternalAccess	HIGH (ALTO)

Impacto

Essas regras tentam detectar mudanças que podem interromper ou destruir dados e recursos, como configurar objetos do Amazon S3 para expirar rapidamente ou permitir o envio do Amazon SES.

Tipo de descoberta	Nome da regra	Gravidade
Impact:S3/DataDestruction	S3LifecycleRapidExpiration	MÉDIO
Impact:SES/ResourceHijacking	SESAccountSendingEnabled	BAIXO
	SESProductionAccessEnabled	MÉDIO

Acesso inicial

Essas regras tentam detectar atividades que abrem acesso ao seu ambiente, como um login no console sem MFA ou tornar um banco de dados do Amazon RDS acessível ao público.

Tipo de descoberta	Nome da regra	Gravidade
InitialAccess:IAM/ValidAccounts	ConsoleLoginWithoutMFA	MÉDIO
InitialAccess:RDS/ExploitPublicFacingApplication	RDSPubliclyAccessible	HIGH (ALTO)

Movimento lateral

Essas regras tentam detectar atividades que concedem acesso entre recursos, como enviar uma chave SSH para uma instância do Amazon EC2.

Tipo de descoberta	Nome da regra	Gravidade
LateralMovement:EC2/RemoteServices	EC2InstanceSSHKeyPushed	MÉDIO

Persistência

Essas regras tentam detectar alterações que criam ou ampliam o acesso, como criar chaves de acesso do IAM, modificar uma política de confiança de funções ou tornar uma função Lambda acessível ao público.

Tipo de descoberta	Nome da regra	Gravidade
Persistence:EC2/BootOrLogonInitializationScripts	EC2UserDataModified	HIGH (ALTO)
Persistence:EC2/ExternalRemoteServices	EC2SecurityGroupPublicSSH	MÉDIO
Persistence:IAM/AccountManipulation	IAMAccessKeyCreated	BAIXO
	IAMRoleTrustPolicyModified	MÉDIO
	IAMUserLoginProfileCreated	HIGH (ALTO)
	IAMUserLoginProfileUpdated	MÉDIO

Tipo de descoberta	Nome da regra	Gravidade
Persistence:Lambda/AccountManipulation	LambdaFunctionPublicAccess	HIGH (ALTO)
Persistence:Lambda/ModifyAuthenticationProcess	LambdaFunctionUrlPublicAccess	HIGH (ALTO)
Persistence:RolesAnywhere/AccountManipulation	RolesAnywhereTrustAnchorCreated	MÉDIO

Escalonamento de privilégios

Essas regras tentam detectar alterações que concedem permissões mais amplas, como anexar uma política de administrador a um usuário ou função do IAM.

Tipo de descoberta	Nome da regra	Gravidade
PrivilegeEscalation:IAM/AccountManipulation	AdminPolicyAttachedToRole	HIGH (ALTO)
	AdminPolicyAttachedToUser	HIGH (ALTO)
	BedrockServiceCredentialCreated	MÉDIO
	SESFullAccessPolicyAttachedToRole	MÉDIO
	SESFullAccessPolicyAttachedToUser	MÉDIO

Desenvolvimento de recursos

Essas regras tentam detectar a configuração de recursos que poderiam apoiar atividades posteriores, como a verificação da identidade de um domínio do Amazon SES.

Tipo de descoberta	Nome da regra	Gravidade
ResourceDevelopment:SES/CompromiseAccounts	SESDomainIdentityVerified	MÉDIO

Regras de detecção personalizadas para monitoramento de tempo de execução

GuardDuty gera os seguintes tipos de regras de detecção personalizadas a partir de sinais de monitoramento de tempo de execução, organizados por MITRE ATT&CK® tactic. Essas regras exigem o Runtime Monitoring e o agente de GuardDuty segurança no recurso monitorado. Para obter mais informações, consulte Fontes de dados e sinais.

Comando e controle

Essas regras tentam detectar processos que encapsulam o tráfego de rede, como ferramentas de tunelamento de DNS ou tunelamento de protocolos.

Tipo de descoberta	Nome da regra	Gravidade
CommandAndControl:Runtime/SuspiciousCommand	DnsTunnelingToolExecuted	HIGH (ALTO)
CommandAndControl:Runtime/SuspiciousCommand	SuspiciousProtocolTunneling	MÉDIO

Acesso credencial

Essas regras tentam detectar processos que leem dados confidenciais, como memória de processo por meio do sistema de `/proc` arquivos.

Tipo de descoberta	Nome da regra	Gravidade
CredentialAccess:Runtime/SensitiveFileRead	DumpProcessMemoryFromProc	HIGH (ALTO)

Deficiência de defesa

Essas regras tentam detectar processos que enfraquecem as defesas do host, como desabilitar o registro de auditoria, modificar regras de firewall ou interromper serviços.

Tipo de descoberta	Nome da regra	Gravidade
DefenseEvasion:Runtime/SensitiveFileModified	FirewallConfigModified	MÉDIO
DefenseEvasion:Runtime/SensitiveFileModified	LogManipulation	MÉDIO
DefenseEvasion:Runtime/SuspiciousCommand	AuditDisabled	MÉDIO
DefenseEvasion:Runtime/SuspiciousCommand	FirewallDisablement	MÉDIO
DefenseEvasion:Runtime/SuspiciousCommand	KernelHardeningDisabled	MÉDIO
DefenseEvasion:Runtime/SuspiciousCommand	KillCommandUsage	MÉDIO
DefenseEvasion:Runtime/SuspiciousCommand	ServiceStoppedOrDisabled	MÉDIO

Descoberta

Essas regras tentam detectar processos que coletam informações sobre um recurso, como ler arquivos de senha, pesquisar credenciais ou chaves ou detectar virtualização.

Tipo de descoberta	Nome da regra	Gravidade
Discovery:Runtime/SensitiveFileRead	PasswordShadowFileDiscovery	MÉDIO
Discovery:Runtime/SuspiciousCommand	FindCommandReconCloudCredentials	MÉDIO
Discovery:Runtime/SuspiciousCommand	FindCommandReconKeyMaterial	MÉDIO
Discovery:Runtime/SuspiciousCommand	PromiscuousModeEnabled	MÉDIO
Discovery:Runtime/SuspiciousCommand	SSHWithHostKeyCheckingDisabled	MÉDIO

Tipo de descoberta	Nome da regra	Gravidade
Discovery:Runtime/SuspiciousCommand	SqliteDatabaseDump	BAIXO
Discovery:Runtime/SuspiciousCommand	VirtualizationDetection	BAIXO

Execução

Essas regras tentam detectar processos que executam comandos ou códigos que podem ser maliciosos, como baixar e executar um script ou abrir um shell interativo em um contêiner.

Tipo de descoberta	Nome da regra	Gravidade
Execution:Runtime/SuspiciousCommand	ChmodInTmpDirectory	MÉDIO
Execution:Runtime/SuspiciousCommand	CurlWgetScriptDownload	MÉDIO
Execution:Runtime/SuspiciousCommand	DataEncryptionUsingCommandLineUtilities	MÉDIO
Execution:Runtime/SuspiciousCommand	InlinePythonExecution	MÉDIO
Execution:Runtime/SuspiciousCommand	InteractiveShellInsideAContainer	MÉDIO
Execution:Runtime/SuspiciousCommand	RemoteFileCopy	MÉDIO
Execution:Runtime/SuspiciousCommand	ShellFromUtilities	MÉDIO
Execution:Runtime/SuspiciousTool	NetworkSnifferToolExecuted	MÉDIO
Execution:Runtime/SuspiciousTool	RawSocketCreated	MÉDIO

Exfiltration

Essas regras tentam detectar processos que movem dados para fora de um recurso, como carregar arquivos com curl, wget ou rclone ou dividir dados antes da transferência.

Tipo de descoberta	Nome da regra	Gravidade
Exfiltration:Runtime/SuspiciousCommand	CurlWgetExfiltrateData	MÉDIO
Exfiltration:Runtime/SuspiciousCommand	DataSplittingForExfiltration	MÉDIO
Exfiltration:Runtime/SuspiciousCommand	S3DataExfiltrationWithRclone	MÉDIO

Persistência

Essas regras tentam detectar alterações que mantêm o acesso a um recurso, como modificar contas de usuário, chaves SSH autorizadas, trabalhos agendados ou serviços do sistema.

Tipo de descoberta	Nome da regra	Gravidade
Persistence:Runtime/SensitiveFileModified	PAMConfigModification	MÉDIO
Persistence:Runtime/SensitiveFileModified	PasswordModification	MÉDIO
Persistence:Runtime/SensitiveFileModified	SSHAuthorizedKeysModification	MÉDIO
Persistence:Runtime/SensitiveFileModified	ScheduledJobManipulation	MÉDIO
Persistence:Runtime/SensitiveFileModified	ShellRCFileManipulated	MÉDIO
Persistence:Runtime/SensitiveFileModified	SystemdServiceManipulation	MÉDIO
Persistence:Runtime/SuspiciousCommand	AuditdKeylogger	MÉDIO
Persistence:Runtime/SuspiciousCommand	InteractiveLocalAccountCreation	MÉDIO
Persistence:Runtime/SuspiciousCommand	NobodyUserManipulation	HIGH (ALTO)
Persistence:Runtime/SuspiciousCommand	SshFromPublicIPAddress	MÉDIO
Persistence:Runtime/SuspiciousCommand	SystemdTransientServiceCreated	MÉDIO

Escalonamento de privilégios

Essas regras tentam detectar alterações que concedem permissões de nível superior, como modificar arquivos sudoers, definir o sinalizador setuid ou escapar de um contêiner com nsenter.

Tipo de descoberta	Nome da regra	Gravidade
DefenseEvasion:Runtime/SuspiciousCommand	FindCommandReconSetuidSetgidFiles	MÉDIO
PrivilegeEscalation:Runtime/SensitiveFileModified	SudoerFileLinked	MÉDIO
PrivilegeEscalation:Runtime/SensitiveFileModified	SudoerFileManipulation	MÉDIO
PrivilegeEscalation:Runtime/SensitiveFileModified	SudoerFileRenamed	MÉDIO
PrivilegeEscalation:Runtime/SuspiciousCommand	AddSetUIDCapability	HIGH (ALTO)
PrivilegeEscalation:Runtime/SuspiciousCommand	NewUserAddedToRootGroup	HIGH (ALTO)
PrivilegeEscalation:Runtime/SuspiciousCommand	NsenterContainerEscape	HIGH (ALTO)
PrivilegeEscalation:Runtime/SuspiciousCommand	SetUidFlagSet	MÉDIO
PrivilegeEscalation:Runtime/SuspiciousCommand	SudoPrivilegeEnumeration	MÉDIO
PrivilegeEscalation:Runtime/SuspiciousCommand	SudoerFileRead	MÉDIO

Stealth

Essas regras tentam detectar processos que ocultam atividades, como sequestrar funções de biblioteca com LD_PRELOAD ou codificar dados com Base64.

Tipo de descoberta	Nome da regra	Gravidade
DefenseEvasion:Runtime/SensitiveFileModified	LDPreloadFunctionHijack	MÉDIO
DefenseEvasion:Runtime/SuspiciousCommand	Base64EncodeDecode	MÉDIO
DefenseEvasion:Runtime/SuspiciousCommand	BpftoolProgramLoaded	MÉDIO
DefenseEvasion:Runtime/SuspiciousCommand	DebugfsRawDiskAccess	MÉDIO
DefenseEvasion:Runtime/SuspiciousCommand	SuspiciousExecutionPath	MÉDIO

GuardDuty Tipos de localização do S3 Protection

As descobertas a seguir são específicas dos recursos do Amazon S3 e terão um tipo de recurso `S3Bucket` se a fonte de dados for eventos de CloudTrail dados para o S3 ou `AccessKey` se a fonte de dados for eventos CloudTrail de gerenciamento. A gravidade e os detalhes das descobertas serão diferentes com base no tipo de descoberta e na permissão associada ao bucket.

As descobertas listadas aqui incluem as fontes de dados e os modelos usados para gerar esse tipo de descoberta. Para obter mais informações sobre modelos e fontes de dados, consulte GuardDuty fontes de dados fundamentais.

> **Important**
>
> As descobertas com uma fonte de dados de eventos de CloudTrail dados para o S3 só são geradas se você tiver ativado o S3 Protection. Por padrão, após 31 de julho de 2020, o S3 Protection é ativado quando uma conta é ativada GuardDuty pela primeira vez ou quando uma conta de GuardDuty administrador delegado é ativada GuardDuty em uma conta de membro existente. No entanto, quando um novo membro ingressa na GuardDuty organização, as preferências de ativação automática da organização serão aplicadas. Para obter informações sobre preferências de ativação automática, consulte Como configurar as

preferências de habilitação automática da organização. Para obter informações sobre como habilitar a proteção do S3, consulte GuardDuty Proteção S3.

Para todos os `S3Bucket` tipos de descobertas, é recomendável que você examine as permissões no bucket em questão e as permissões de qualquer usuário envolvido na descoberta. Se a atividade for inesperada, consulte as recomendações de remediação detalhadas emComo corrigir um bucket do S3 possivelmente comprometido.

Tópicos

- Discovery:S3/AnomalousBehavior
- Discovery:S3/MaliciousIPCaller
- Discovery:S3/MaliciousIPCaller.Custom
- Discovery:S3/TorIPCaller
- Exfiltration:S3/AnomalousBehavior
- Exfiltration:S3/MaliciousIPCaller
- Impact:S3/AnomalousBehavior.Delete
- Impact:S3/AnomalousBehavior.Permission
- Impact:S3/AnomalousBehavior.Write
- Impact:S3/MaliciousIPCaller
- PenTest:S3/KaliLinux
- PenTest:S3/ParrotLinux
- PenTest:S3/PentooLinux
- Policy:S3/AccountBlockPublicAccessDisabled
- Policy:S3/BucketAnonymousAccessGranted
- Policy:S3/BucketBlockPublicAccessDisabled
- Policy:S3/BucketPublicAccessGranted
- Stealth:S3/ServerAccessLoggingDisabled
- UnauthorizedAccess:S3/MaliciousIPCaller.Custom
- UnauthorizedAccess:S3/TorIPCaller

Discovery:S3/AnomalousBehavior

Uma API comumente usada para descobrir objetos do S3 foi invocada de forma anômala.

Gravidade padrão: baixa

- Fonte de dados: eventos CloudTrail de dados para S3

Essa descoberta informa que uma entidade do IAM invocou uma API do S3 para descobrir buckets do S3 em seu ambiente, como `ListObjects`. Esse tipo de atividade está associado ao estágio de descoberta de um ataque, no qual um invasor coleta informações para determinar se seu AWS ambiente é suscetível a um ataque mais amplo. Essa atividade é suspeita porque a entidade do IAM invocou a API de uma forma incomum. Por exemplo, uma entidade do IAM sem histórico anterior invoca uma API do S3, ou uma entidade do IAM invoca uma API do S3 de um local incomum.

Essa API foi identificada como anômala pelo modelo de aprendizado GuardDuty de máquina (ML) de detecção de anomalias. O modelo de ML avalia todas as solicitações de API em sua conta e identifica eventos anômalos associados às técnicas usadas pelos adversários. Ele rastreia vários fatores das solicitações de API, como o usuário que fez a solicitação, o local de onde a solicitação foi feita, a API específica solicitada, o bucket solicitado e o número de chamadas de API feitas. Para obter mais informações sobre quais fatores da solicitação de API são incomuns para a identidade do usuário que invocou a solicitação, consulte Como encontrar detalhes.

Recomendações de correção:

Se essa atividade for inesperada para a entidade principal associada, isso pode indicar que as credenciais foram expostas ou que suas permissões do S3 não são restritivas o suficiente. Para obter mais informações, consulte Como corrigir um bucket do S3 possivelmente comprometido.

Discovery:S3/MaliciousIPCaller

Uma API do S3 comumente usada para descobrir recursos em um AWS o ambiente foi invocado a partir de um endereço IP malicioso conhecido.

Gravidade padrão: alta

- Fonte de dados: eventos CloudTrail de dados para S3

Essa descoberta informa que uma operação da API S3 foi invocada a partir de um endereço IP associado a atividades mal-intencionadas conhecidas. A API observada geralmente está associada ao estágio de descoberta de um ataque, quando um adversário está coletando informações sobre seu AWS ambiente. Exemplos incluem `GetObjectAcl` e `ListObjects`.

Recomendações de correção:

Se essa atividade for inesperada para a entidade principal associada, isso pode indicar que as credenciais foram expostas ou que suas permissões do S3 não são restritivas o suficiente. Para obter mais informações, consulte Como corrigir um bucket do S3 possivelmente comprometido.

Discovery:S3/MaliciousIPCaller.Custom

Uma API do S3 foi invocada a partir de um endereço IP em uma lista de ameaças personalizada.

Gravidade padrão: alta

- Fonte de dados: eventos CloudTrail de dados para S3

Essa descoberta informa que uma API do S3, como `GetObjectAcl` ou `ListObjects`, foi invocada de um endereço IP incluído em uma lista de ameaças que você carregou. A lista de ameaças associada a essa descoberta está listada na seção Informações adicionais dos detalhes de uma descoberta. Esse tipo de atividade está associado ao estágio de descoberta de um ataque, no qual um invasor coleta informações para determinar se seu AWS ambiente é suscetível a um ataque mais amplo.

Recomendações de correção:

Se essa atividade for inesperada para a entidade principal associada, isso pode indicar que as credenciais foram expostas ou que suas permissões do S3 não são restritivas o suficiente. Para obter mais informações, consulte Como corrigir um bucket do S3 possivelmente comprometido.

Discovery:S3/TorIPCaller

Uma API do S3 foi invocada a partir de um endereço IP do nó de saída do Tor.

Gravidade padrão: média

- Fonte de dados: eventos CloudTrail de dados para S3

Essa descoberta informa que uma API do S3, como `GetObjectAcl` ou `ListObjects`, foi invocada a partir de um endereço IP do nó de saída do Tor. Esse tipo de atividade está associado ao estágio de descoberta de um ataque, no qual um atacante coleta informações para determinar se seu AWS ambiente é suscetível a um ataque mais amplo. Tor é um software para permitir a comunicação anônima. Ele criptografa e aleatoriamente envia comunicações por meio de relés entre uma série de nós de rede. O último nó do Tor é chamado de nó de saída. Isso pode indicar acesso não autorizado aos seus AWS recursos com a intenção de ocultar a verdadeira identidade do atacante.

Recomendações de correção:

Se essa atividade for inesperada para a entidade principal associada, isso pode indicar que as credenciais foram expostas ou que suas permissões do S3 não são restritivas o suficiente. Para obter mais informações, consulte Como corrigir um bucket do S3 possivelmente comprometido.

Exfiltration:S3/AnomalousBehavior

Uma entidade do IAM invocou uma API do S3 de forma suspeita.

Gravidade padrão: alta

- Fonte de dados: eventos CloudTrail de dados para S3

Essa descoberta informa que uma entidade do IAM está fazendo chamadas de API que envolvem um bucket do S3 e essa atividade é diferente da linha de base estabelecida pela entidade. A chamada de API usada nessa atividade está associada ao estágio de exfiltração de um ataque, no qual um invasor tenta coletar dados. Essa atividade é suspeita porque a entidade do IAM invocou a API de uma forma incomum. Por exemplo, uma entidade do IAM sem histórico anterior invoca uma API do S3, ou uma entidade do IAM invoca uma API do S3 de um local incomum.

Essa API foi identificada como anômala pelo modelo de aprendizado GuardDuty de máquina (ML) de detecção de anomalias. O modelo de ML avalia todas as solicitações de API em sua conta e identifica eventos anômalos associados às técnicas usadas pelos adversários. Ele rastreia vários fatores das solicitações de API, como o usuário que fez a solicitação, o local de onde a solicitação foi feita, a API específica solicitada, o bucket solicitado e o número de chamadas de API feitas. Para obter mais informações sobre quais fatores da solicitação de API são incomuns para a identidade do usuário que invocou a solicitação, consulte Como encontrar detalhes.

Recomendações de correção:

Se essa atividade for inesperada para a entidade principal associada, isso pode indicar que as credenciais foram expostas ou que suas permissões do S3 não são restritivas o suficiente. Para obter mais informações, consulte Como corrigir um bucket do S3 possivelmente comprometido.

Exfiltration:S3/MaliciousIPCaller

Uma API do S3 comumente usada para coletar dados de um AWS o ambiente foi invocado a partir de um endereço IP malicioso conhecido.

Gravidade padrão: alta

- Fonte de dados: eventos CloudTrail de dados para S3

Essa descoberta informa que uma operação da API S3 foi invocada a partir de um endereço IP associado a atividades mal-intencionadas conhecidas. Comumente, a API observada é associada a táticas de exfiltração em que um adversário está tentando coletar dados da sua rede. Exemplos incluem `GetObject` e `CopyObject`.

Recomendações de correção:

Se essa atividade for inesperada para a entidade principal associada, isso pode indicar que as credenciais foram expostas ou que suas permissões do S3 não são restritivas o suficiente. Para obter mais informações, consulte Como corrigir um bucket do S3 possivelmente comprometido.

Impact:S3/AnomalousBehavior.Delete

Uma entidade do IAM invocou uma API do S3 que tenta excluir dados de forma suspeita.

Gravidade padrão: alta

- Fonte de dados: eventos CloudTrail de dados para S3

Essa descoberta informa que uma entidade do IAM em seu AWS ambiente está fazendo chamadas de API que envolvem um bucket do S3, e esse comportamento difere da linha de base estabelecida pela entidade. A chamada de API usada nessa atividade está associada a um ataque que tenta excluir dados. Essa atividade é suspeita porque a entidade do IAM invocou a API de uma forma

incomum. Por exemplo, uma entidade do IAM sem histórico anterior invoca uma API do S3, ou uma entidade do IAM invoca uma API do S3 de um local incomum.

Essa API foi identificada como anômala pelo modelo de aprendizado GuardDuty de máquina (ML) de detecção de anomalias. O modelo de ML avalia todas as solicitações de API em sua conta e identifica eventos anômalos associados às técnicas usadas pelos adversários. Ele rastreia vários fatores das solicitações de API, como o usuário que fez a solicitação, o local de onde a solicitação foi feita, a API específica solicitada, o bucket solicitado e o número de chamadas de API feitas. Para obter mais informações sobre quais fatores da solicitação de API são incomuns para a identidade do usuário que invocou a solicitação, consulte Como encontrar detalhes.

Recomendações de correção:

Se essa atividade for inesperada para a entidade principal associada, isso pode indicar que as credenciais foram expostas ou que suas permissões do S3 não são restritivas o suficiente. Para obter mais informações, consulte Como corrigir um bucket do S3 possivelmente comprometido.

Recomendamos uma auditoria do conteúdo do seu bucket do S3 para determinar se a versão anterior do objeto pode ou deve ser restaurada.

Impact:S3/AnomalousBehavior.Permission

Uma API comumente usada para definir as permissões de lista de controle de acesso (ACL) foi invocada de forma anômala.

Gravidade padrão: alta

- Fonte de dados: eventos CloudTrail de dados para S3

Essa descoberta informa que uma entidade do IAM em seu AWS ambiente atualizou uma política de bucket ou ACL nos buckets do S3 listados. Essa alteração pode expor publicamente seus buckets do S3 a todos os usuários autenticados. AWS

Essa API foi identificada como anômala pelo modelo de aprendizado GuardDuty de máquina (ML) de detecção de anomalias. O modelo de ML avalia todas as solicitações de API em sua conta e identifica eventos anômalos associados às técnicas usadas pelos adversários. Ele rastreia vários fatores das solicitações de API, como o usuário que fez a solicitação, o local de onde a solicitação foi feita, a API específica solicitada, o bucket solicitado e o número de chamadas de API feitas. Para obter mais informações sobre quais fatores da solicitação de API são incomuns para a identidade do usuário que invocou a solicitação, consulte Como encontrar detalhes.

Recomendações de correção:

Se essa atividade for inesperada para a entidade principal associada, isso pode indicar que as credenciais foram expostas ou que suas permissões do S3 não são restritivas o suficiente. Para obter mais informações, consulte Como corrigir um bucket do S3 possivelmente comprometido.

Recomendamos uma auditoria do conteúdo do seu bucket do S3 para garantir que nenhum objeto tenha permissão inesperada para ser acessado publicamente.

Impact:S3/AnomalousBehavior.Write

Uma entidade do IAM invocou uma API do S3 que tenta gravar dados de forma suspeita.

Gravidade padrão: média

- Fonte de dados: eventos CloudTrail de dados para S3

Essa descoberta informa que uma entidade do IAM em seu AWS ambiente está fazendo chamadas de API que envolvem um bucket do S3, e esse comportamento difere da linha de base estabelecida pela entidade. A chamada de API usada nessa atividade está associada a um ataque que tenta gravar dados. Essa atividade é suspeita porque a entidade do IAM invocou a API de uma forma incomum. Por exemplo, uma entidade do IAM sem histórico anterior invoca uma API do S3, ou uma entidade do IAM invoca uma API do S3 de um local incomum.

Essa API foi identificada como anômala pelo modelo de aprendizado GuardDuty de máquina (ML) de detecção de anomalias. O modelo de ML avalia todas as solicitações de API em sua conta e identifica eventos anômalos associados às técnicas usadas pelos adversários. Ele rastreia vários fatores das solicitações de API, como o usuário que fez a solicitação, o local de onde a solicitação foi feita, a API específica solicitada, o bucket solicitado e o número de chamadas de API feitas. Para obter mais informações sobre quais fatores da solicitação de API são incomuns para a identidade do usuário que invocou a solicitação, consulte Como encontrar detalhes.

Recomendações de correção:

Se essa atividade for inesperada para a entidade principal associada, isso pode indicar que as credenciais foram expostas ou que suas permissões do S3 não são restritivas o suficiente. Para obter mais informações, consulte Como corrigir um bucket do S3 possivelmente comprometido.

Recomendamos uma auditoria do conteúdo do seu bucket do S3 para garantir que essa chamada de API não tenha gravado dados mal-intencionados ou não autorizados.

Impact:S3/MaliciousIPCaller

Uma API do S3 comumente usada para adulterar dados ou processos em um AWS o ambiente foi invocado a partir de um endereço IP malicioso conhecido.

Gravidade padrão: alta

- Fonte de dados: eventos CloudTrail de dados para S3

Essa descoberta informa que uma operação da API S3 foi invocada a partir de um endereço IP associado a atividades mal-intencionadas conhecidas. A API observada é comumente associada a táticas de impacto em que um adversário está tentando manipular, interromper ou destruir dados em seu ambiente. AWS Exemplos incluem `PutObject` e `PutObjectAcl`.

Recomendações de correção:

Se essa atividade for inesperada para a entidade principal associada, isso pode indicar que as credenciais foram expostas ou que suas permissões do S3 não são restritivas o suficiente. Para obter mais informações, consulte Como corrigir um bucket do S3 possivelmente comprometido.

PenTest:S3/KaliLinux

Uma API do S3 foi invocada de uma máquina Linux Kali.

Gravidade padrão: média

- Fonte de dados: eventos CloudTrail de dados para S3

Essa descoberta informa que uma máquina executando o Kali Linux está fazendo chamadas de API do S3 usando credenciais que pertencem à sua conta. AWS Suas credenciais podem estar comprometidas. O Kali Linux é uma ferramenta conhecida de teste de penetração usada por profissionais de segurança para identificar vulnerabilidades em instâncias do EC2 que exigem correções. Os invasores também usam essa ferramenta para encontrar pontos fracos na configuração do EC2 e obter acesso não autorizado ao seu ambiente. AWS

Recomendações de correção:

Se essa atividade for inesperada para a entidade principal associada, isso pode indicar que as credenciais foram expostas ou que suas permissões do S3 não são restritivas o suficiente. Para obter mais informações, consulte Como corrigir um bucket do S3 possivelmente comprometido.

PenTest:S3/ParrotLinux

Uma API do S3 foi invocada a partir de uma máquina Parrot Security Linux.

Gravidade padrão: média

- Fonte de dados: eventos CloudTrail de dados para S3

Essa descoberta informa que uma máquina executando o Parrot Security Linux está fazendo chamadas de API do S3 usando credenciais que pertencem à sua conta. AWS Suas credenciais podem estar comprometidas. O Parrot Security Linux é uma ferramenta popular de teste de penetração que profissionais de segurança usam para identificar vulnerabilidades nas instâncias do EC2 que exigem correções. Os invasores também usam essa ferramenta para encontrar vulnerabilidades na configuração do EC2 e obter acesso não autorizado ao seu ambiente da AWS .

Recomendações de correção:

Se essa atividade for inesperada para a entidade principal associada, isso pode indicar que as credenciais foram expostas ou que suas permissões do S3 não são restritivas o suficiente. Para obter mais informações, consulte Como corrigir um bucket do S3 possivelmente comprometido.

PenTest:S3/PentooLinux

Uma API do S3 foi invocada de uma máquina Linux Pentoo.

Gravidade padrão: média

- Fonte de dados: eventos CloudTrail de dados para S3

Essa descoberta informa que uma máquina executando o Pentoo Linux está fazendo chamadas de API do S3 usando credenciais que pertencem à sua conta. AWS Suas credenciais podem estar comprometidas. O Pentoo Linux é uma ferramenta conhecida de teste de penetração usada por profissionais de segurança para identificar vulnerabilidades em instâncias do EC2 que exigem correções. Os invasores também usam essa ferramenta para encontrar pontos fracos na configuração do EC2 e obter acesso não autorizado ao seu ambiente. AWS

Recomendações de correção:

Se essa atividade for inesperada para a entidade principal associada, isso pode indicar que as credenciais foram expostas ou que suas permissões do S3 não são restritivas o suficiente. Para obter mais informações, consulte Como corrigir um bucket do S3 possivelmente comprometido.

Policy:S3/AccountBlockPublicAccessDisabled

Uma entidade do IAM invocou uma API usada para desabilitar o Bloqueio de acesso público do S3 em uma conta.

Gravidade padrão: baixa

- Fonte de dados: eventos CloudTrail de gerenciamento

Essa descoberta informa que o Amazon S3 Block Public Access foi desabilitado no nível da conta. Quando as configurações de bloqueio de acesso público do S3 são usadas para filtrar as políticas ou listas de controle de acesso (ACLs) aplicadas ao bucket para evitar a exposição pública acidental de dados.

Normalmente, o bloqueio de acesso público do S3 é desabilitado para permitir o acesso público a um bucket ou aos objetos no bucket. Quando o S3 Block Public Access é desabilitado para uma conta, o acesso aos seus buckets é controlado pelas políticas, ACLs ou configurações de Block Public Access em nível de bucket aplicadas aos seus buckets individuais. Isso não significa necessariamente que os buckets são compartilhados publicamente, mas que você deve auditar as permissões aplicadas aos buckets para confirmar que eles fornecem o nível apropriado de acesso.

Recomendações de correção:

Se essa atividade for inesperada para a entidade principal associada, isso pode indicar que as credenciais foram expostas ou que suas permissões do S3 não são restritivas o suficiente. Para obter mais informações, consulte Como corrigir um bucket do S3 possivelmente comprometido.

Policy:S3/BucketAnonymousAccessGranted

Uma entidade principal do IAM concedeu acesso a um bucket do S3 na Internet alterando as políticas do bucket ou as ACLs.

Gravidade padrão: alta

- Fonte de dados: eventos CloudTrail de gerenciamento

Essa descoberta informa que o bucket do S3 listado se tornou acessível publicamente na Internet porque uma entidade do IAM alterou uma política de bucket ou ACL nesse bucket.

Depois que uma alteração na política ou na ACL é detectada, GuardDuty usa o raciocínio automatizado desenvolvido pela Zelkova para determinar se o bucket está acessível ao público.

> **Note**
>
> Se as ACLs ou políticas de bucket de um bucket estiverem configuradas para negar explicitamente ou negar tudo, essa descoberta pode não refletir o estado atual do bucket. Essa descoberta não refletirá nenhuma configuração de Bloqueio de acesso público do S3 que possa ter sido habilitada para seu bucket do S3. Nesses casos, o valor de `effectivePermission` na descoberta será marcado como `UNKNOWN`.

Recomendações de correção:

Se essa atividade for inesperada para a entidade principal associada, isso pode indicar que as credenciais foram expostas ou que suas permissões do S3 não são restritivas o suficiente. Para obter mais informações, consulte Como corrigir um bucket do S3 possivelmente comprometido.

Policy:S3/BucketBlockPublicAccessDisabled

Uma entidade principal do IAM invocou uma API usada para desabilitar o bloqueio de acesso público do S3 em um bucket.

Gravidade padrão: baixa

- Fonte de dados: eventos CloudTrail de gerenciamento

Essa descoberta informa que o Bloqueio de acesso público foi desabilitado para o bucket do S3 listado. Quando habilitadas, as configurações do Bloqueio de acesso público do S3 são usadas para filtrar as políticas ou as listas de controle de acesso (ACLs) aplicadas aos buckets para evitar a exposição pública acidental de dados.

Normalmente, o bloqueio de acesso público do S3 é desabilitado para permitir o acesso público a um bucket ou aos objetos no bucket. Quando o Bloqueio de acesso público do S3 é desabilitado

para um bucket, o acesso ao bucket é controlado pelas políticas ou ACLs aplicados a ele. Isso não significa que o bucket seja compartilhado publicamente, mas você deve auditar as políticas e ACLs aplicadas ao bucket para confirmar se as permissões apropriadas foram aplicadas.

Recomendações de correção:

Se essa atividade for inesperada para a entidade principal associada, isso pode indicar que as credenciais foram expostas ou que suas permissões do S3 não são restritivas o suficiente. Para obter mais informações, consulte Como corrigir um bucket do S3 possivelmente comprometido.

Policy:S3/BucketPublicAccessGranted

Um diretor do IAM concedeu acesso público a um bucket do S3 para todos AWS usuários alterando as políticas de bucket ou as ACLs.

Gravidade padrão: alta

- Fonte de dados: eventos CloudTrail de gerenciamento

Essa descoberta informa que o bucket do S3 listado foi exposto publicamente a todos os AWS usuários autenticados porque uma entidade do IAM alterou uma política de bucket ou ACL nesse bucket do S3.

Depois que uma alteração na política ou na ACL é detectada, GuardDuty usa o raciocínio automatizado desenvolvido pela Zelkova para determinar se o bucket está acessível ao público.

> **Note**
>
> Se as ACLs ou políticas de bucket de um bucket estiverem configuradas para negar explicitamente ou negar tudo, essa descoberta pode não refletir o estado atual do bucket. Essa descoberta não refletirá nenhuma configuração de Bloqueio de acesso público do S3 que possa ter sido habilitada para seu bucket do S3. Nesses casos, o valor de `effectivePermission` na descoberta será marcado como `UNKNOWN`.

Recomendações de correção:

Se essa atividade for inesperada para a entidade principal associada, isso pode indicar que as credenciais foram expostas ou que suas permissões do S3 não são restritivas o suficiente. Para obter mais informações, consulte Como corrigir um bucket do S3 possivelmente comprometido.

Stealth:S3/ServerAccessLoggingDisabled

O registro em log de acesso ao servidor do S3 foi desabilitado para um bucket

Gravidade padrão: baixa

- Fonte de dados: eventos CloudTrail de gerenciamento

Essa descoberta informa que o registro de acesso ao servidor S3 está desativado para um bucket em seu AWS ambiente. Se desativado, nenhum registro de solicitação da web será criado para qualquer tentativa de acessar o bucket do S3 identificado; no entanto, as chamadas da API de gerenciamento do S3 para o bucket, como DeleteBucket, ainda serão rastreadas. Se o registro de eventos de dados do S3 estiver ativado CloudTrail por meio desse bucket, as solicitações web para objetos dentro do bucket ainda serão rastreadas. Desabilitar o registro em log é uma técnica frequentemente usada por usuários não autorizados para burlar a detecção. Para saber mais sobre os logs do S3, consulte Registro em log de acesso ao servidor do S3 e Opções de registro em log do S3.

Recomendações de correção:

Se essa atividade for inesperada para a entidade principal associada, isso pode indicar que as credenciais foram expostas ou que suas permissões do S3 não são restritivas o suficiente. Para obter mais informações, consulte Como corrigir um bucket do S3 possivelmente comprometido.

UnauthorizedAccess:S3/MaliciousIPCaller.Custom

Uma API do S3 foi invocada a partir de um endereço IP em uma lista de ameaças personalizada.

Gravidade padrão: alta

- Fonte de dados: eventos CloudTrail de dados para S3

Essa descoberta informa que uma operação da API do S3, por exemplo, `PutObject` ou `PutObjectAcl`, foi invocada a partir de um endereço IP incluído em uma lista de ameaças que você carregou. A lista de ameaças associada a essa descoberta está listada na seção Informações adicionais dos detalhes de uma descoberta.

Recomendações de correção:

Se essa atividade for inesperada para a entidade principal associada, isso pode indicar que as credenciais foram expostas ou que suas permissões do S3 não são restritivas o suficiente. Para obter mais informações, consulte Como corrigir um bucket do S3 possivelmente comprometido.

UnauthorizedAccess:S3/TorIPCaller

Uma API do S3 foi invocada a partir de um endereço IP do nó de saída do Tor.

Gravidade padrão: alta

- Fonte de dados: eventos CloudTrail de dados para S3

Essa descoberta informa que uma operação da API do S3, como `PutObject` ou `PutObjectAcl`, foi invocada a partir de um endereço IP do nó de saída do Tor. Tor é um software para permitir a comunicação anônima. Ele criptografa e aleatoriamente envia comunicações por meio de relés entre uma série de nós de rede. O último nó do Tor é chamado de nó de saída. Essa descoberta pode indicar acesso não autorizado aos seus AWS recursos com a intenção de ocultar a verdadeira identidade do atacante.

Recomendações de correção:

Se essa atividade for inesperada para a entidade principal associada, isso pode indicar que as credenciais foram expostas ou que suas permissões do S3 não são restritivas o suficiente. Para obter mais informações, consulte Como corrigir um bucket do S3 possivelmente comprometido.

Tipos de descoberta da Proteção do EKS

As descobertas a seguir são específicas para os recursos do Amazon EKS e têm um resource_type de `EKSCluster`. A gravidade e os detalhes das descobertas serão diferentes com base no tipo de descoberta.

Para todas as descobertas de logs de auditoria EKS recomendamos que você examine o recurso em questão para determinar se a atividade é esperada ou potencialmente mal-intencionada. Para obter orientação sobre como remediar um recurso comprometido de registros de auditoria do EKS identificado por uma GuardDuty descoberta, consulte. Como corrigir as descobertas da Proteção do EKS

> **Note**
>
> Se a atividade pela qual essas descobertas são geradas for esperada, considere adicionar Regras de supressão em GuardDuty para evitar futuros alertas.

Tópicos

- CredentialAccess:Kubernetes/MaliciousIPCaller
- CredentialAccess:Kubernetes/MaliciousIPCaller.Custom
- CredentialAccess:Kubernetes/SuccessfulAnonymousAccess
- CredentialAccess:Kubernetes/TorIPCaller
- DefenseEvasion:Kubernetes/MaliciousIPCaller
- DefenseEvasion:Kubernetes/MaliciousIPCaller.Custom
- DefenseEvasion:Kubernetes/SuccessfulAnonymousAccess
- DefenseEvasion:Kubernetes/TorIPCaller
- Discovery:Kubernetes/MaliciousIPCaller
- Discovery:Kubernetes/MaliciousIPCaller.Custom
- Discovery:Kubernetes/SuccessfulAnonymousAccess
- Discovery:Kubernetes/TorIPCaller
- Execution:Kubernetes/ExecInKubeSystemPod
- Impact:Kubernetes/MaliciousIPCaller
- Impact:Kubernetes/MaliciousIPCaller.Custom
- Impact:Kubernetes/SuccessfulAnonymousAccess
- Impact:Kubernetes/TorIPCaller
- Persistence:Kubernetes/MaliciousIPCaller
- Persistence:Kubernetes/MaliciousIPCaller.Custom
- Persistence:Kubernetes/SuccessfulAnonymousAccess
- Persistence:Kubernetes/TorIPCaller
- Policy:Kubernetes/AdminAccessToDefaultServiceAccount
- Policy:Kubernetes/AnonymousAccessGranted

- Policy:Kubernetes/ExposedDashboard
- Policy:Kubernetes/KubeflowDashboardExposed
- CredentialAccess:Kubernetes/AnomalousBehavior.SecretsAccessed
- PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleBindingCreated
- Execution:Kubernetes/AnomalousBehavior.ExecInPod
- PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!PrivilegedContainer
- Persistence:Kubernetes/AnomalousBehavior.WorkloadDeployed!ContainerWithSensitiveMount
- Execution:Kubernetes/AnomalousBehavior.WorkloadDeployed
- PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleCreated
- Discovery:Kubernetes/AnomalousBehavior.PermissionChecked

> **Note**
>
> Antes da versão 1.14 do Kubernetes, o `system:unauthenticated` grupo era associado e por padrão. `system:discovery` `system:basic-user` ClusterRoles Essa associação pode permitir o acesso não intencional de usuários anônimos. As atualizações do cluster não revogam essas permissões. Mesmo que você tenha atualizado seu cluster para a versão 1.14 ou superior, essas permissões ainda poderão estar habilitadas. Recomendamos que você desassocie essas permissões do grupo `system:unauthenticated`. Para obter orientação sobre a revogação dessas permissões, consulte as Práticas recomendadas de segurança do Amazon EKS no Guia do usuário do Amazon EKS.

CredentialAccess:Kubernetes/MaliciousIPCaller

Uma API comumente usada para acessar credenciais ou segredos em um cluster do Kubernetes foi invocada a partir de um endereço IP mal-intencionado conhecido.

Gravidade padrão: alta

- Funcionalidade: logs de auditoria do EKS

Essa descoberta informa que uma operação de API foi invocada a partir de um endereço IP associado a atividades mal-intencionadas conhecidas. Comumente, a API observada é associada

às táticas de acesso a credenciais em que um adversário está tentando coletar senhas, nomes de usuário e chaves de acesso para seu cluster do Kubernetes.

Recomendações de correção:

Se o usuário relatado na descoberta na seção `KubernetesUserDetails` for `system:anonymous`, investigue por que o usuário anônimo teve permissão para invocar a API e revogue as permissões, se necessário, seguindo as instruções nas Práticas recomendadas de segurança do Amazon EKS no Guia do usuário do Amazon EKS. Se o usuário for um usuário autenticado, investigue para determinar se a atividade foi legítima ou mal-intencionada. Se a atividade for mal-intencionada, revogue o acesso do usuário e reverta as alterações feitas por um adversário no seu cluster. Para obter mais informações, consulte Como corrigir as descobertas da Proteção do EKS.

CredentialAccess:Kubernetes/MaliciousIPCaller.Custom

Uma API comumente usada para acessar credenciais ou segredos em um cluster do Kubernetes foi invocada a partir de um endereço IP em uma lista de ameaças personalizada.

Gravidade padrão: alta

- Funcionalidade: logs de auditoria do EKS

Essa descoberta informa que uma operação de API foi invocada a partir de um endereço IP incluído em uma lista de ameaças que você carregou. A lista de ameaças associada a essa descoberta está listada na seção Informações adicionais dos detalhes de uma descoberta. Comumente, a API observada é associada às táticas de acesso a credenciais em que um adversário está tentando coletar senhas, nomes de usuário e chaves de acesso para seu cluster do Kubernetes.

Recomendações de correção:

Se o usuário relatado na descoberta na seção `KubernetesUserDetails` for `system:anonymous`, investigue por que o usuário anônimo teve permissão para invocar a API e revogue as permissões, se necessário, seguindo as instruções nas Práticas recomendadas de segurança do Amazon EKS no Guia do usuário do Amazon EKS. Se o usuário for um usuário autenticado, investigue para determinar se a atividade foi legítima ou mal-intencionada. Se a atividade for mal-intencionada, revogue o acesso do usuário e reverta as alterações feitas por um adversário no seu cluster. Para obter mais informações, consulte Como corrigir as descobertas da Proteção do EKS.

CredentialAccess:Kubernetes/SuccessfulAnonymousAccess

Uma API comumente usada para acessar credenciais ou segredos em um cluster do Kubernetes foi invocada por um usuário não autenticado.

Gravidade padrão: alta

- Funcionalidade: logs de auditoria do EKS

Essa descoberta informa que uma operação de API foi invocada com sucesso pelo usuário `system:anonymous`. As chamadas de API feitas por `system:anonymous` não são autenticadas. Comumente, a API observada é associada às táticas de acesso a credenciais em que um adversário está tentando coletar senhas, nomes de usuário e chaves de acesso para seu cluster do Kubernetes. Essa atividade indica que o acesso anônimo ou não autenticado é permitido na ação da API relatada na descoberta e pode ser permitido em outras ações. Se esse comportamento não for esperado, isso pode indicar um erro de configuração ou que suas credenciais estão comprometidas.

Recomendações de correção:

Você deve examinar as permissões que foram concedidas ao usuário `system:anonymous` em seu cluster e garantir que todas as permissões sejam necessárias. Se as permissões foram concedidas por engano ou de maneira mal-intencionada, você deve revogar o acesso do usuário e reverter as alterações feitas por um adversário no seu cluster. Para obter mais informações, consulte Práticas recomendadas de segurança para o Amazon EKS no Guia do usuário do Amazon EKS.

Para obter mais informações, consulte Como corrigir as descobertas da Proteção do EKS.

CredentialAccess:Kubernetes/TorIPCaller

Uma API comumente usada para acessar credenciais ou segredos em um cluster do Kubernetes foi invocada a partir de um endereço IP do nó de saída do Tor.

Gravidade padrão: alta

- Funcionalidade: logs de auditoria do EKS

Essa descoberta informa que uma operação da API foi invocada a partir de um endereço IP do nó de saída do Tor. Comumente, a API observada é associada às táticas de acesso a credenciais em

que um adversário está tentando coletar senhas, nomes de usuário e chaves de acesso para seu cluster do Kubernetes. Tor é um software para permitir a comunicação anônima. Ele criptografa e aleatoriamente envia comunicações por meio de relés entre uma série de nós de rede. O último nó do Tor é chamado de nó de saída. Isso pode indicar acesso não autorizado aos recursos do cluster do Kubernetes com a intenção de ocultar a verdadeira identidade do invasor.

Recomendações de correção:

Se o usuário relatado na descoberta na seção `KubernetesUserDetails` for `system:anonymous`, investigue por que o usuário anônimo teve permissão para invocar a API e revogue as permissões, se necessário, seguindo as instruções nas Práticas recomendadas de segurança do Amazon EKS no Guia do usuário do Amazon EKS. Se o usuário for um usuário autenticado, investigue para determinar se a atividade foi legítima ou mal-intencionada. Se a atividade for mal-intencionada, revogue o acesso do usuário e reverta as alterações feitas por um adversário no seu cluster. Para obter mais informações, consulte Como corrigir as descobertas da Proteção do EKS.

DefenseEvasion:Kubernetes/MaliciousIPCaller

Uma API comumente usada para evitar medidas defensivas foi invocada a partir de um endereço IP mal-intencionado conhecido.

Gravidade padrão: alta

- Funcionalidade: logs de auditoria do EKS

Essa descoberta informa que uma operação de API foi invocada a partir de um endereço IP associado a atividades mal-intencionadas conhecidas. Comumente, a API observada é associada a táticas de evasão de defesa, nas quais um adversário está tentando esconder suas ações para evitar a detecção.

Recomendações de correção:

Se o usuário relatado na descoberta na seção `KubernetesUserDetails` for `system:anonymous`, investigue por que o usuário anônimo teve permissão para invocar a API e revogue as permissões, se necessário, seguindo as instruções nas Práticas recomendadas de segurança do Amazon EKS no Guia do usuário do Amazon EKS. Se o usuário for um usuário autenticado, investigue para determinar se a atividade foi legítima ou mal-intencionada. Se a atividade for mal-intencionada, revogue o acesso do usuário e reverta as alterações feitas por um adversário no seu cluster. Para obter mais informações, consulte Como corrigir as descobertas da Proteção do EKS.

DefenseEvasion:Kubernetes/MaliciousIPCaller.Custom

Uma API foi invocada a partir de um endereço IP em uma lista de ameaças personalizada.

Gravidade padrão: alta

- Funcionalidade: logs de auditoria do EKS

Essa descoberta informa que uma operação de API foi invocada a partir de um endereço IP incluído em uma lista de ameaças que você carregou. A lista de ameaças associada a essa descoberta está listada na seção Informações adicionais dos detalhes de uma descoberta. Comumente, a API observada é associada a táticas de evasão de defesa, nas quais um adversário está tentando esconder suas ações para evitar a detecção.

Recomendações de correção:

Se o usuário relatado na descoberta na seção `KubernetesUserDetails` for `system:anonymous`, investigue por que o usuário anônimo teve permissão para invocar a API e revogue as permissões, se necessário, seguindo as instruções nas Práticas recomendadas de segurança do Amazon EKS no Guia do usuário do Amazon EKS. Se o usuário for um usuário autenticado, investigue para determinar se a atividade foi legítima ou mal-intencionada. Se a atividade for mal-intencionada, revogue o acesso do usuário e reverta as alterações feitas por um adversário no seu cluster. Para obter mais informações, consulte Como corrigir as descobertas da Proteção do EKS.

DefenseEvasion:Kubernetes/SuccessfulAnonymousAccess

Uma API comumente usada para evitar medidas defensivas foi invocada por um usuário não autenticado.

Gravidade padrão: alta

- Funcionalidade: logs de auditoria do EKS

Essa descoberta informa que uma operação de API foi invocada com sucesso pelo usuário `system:anonymous`. As chamadas de API feitas por `system:anonymous` não são autenticadas. Comumente, a API observada é associada a táticas de evasão de defesa, nas quais um adversário está tentando esconder suas ações para evitar a detecção. Essa atividade indica que o acesso

anônimo ou não autenticado é permitido na ação da API relatada na descoberta e pode ser permitido em outras ações. Se esse comportamento não for esperado, isso pode indicar um erro de configuração ou que suas credenciais estão comprometidas.

Recomendações de correção:

Você deve examinar as permissões que foram concedidas ao usuário `system:anonymous` em seu cluster e garantir que todas as permissões sejam necessárias. Se as permissões foram concedidas por engano ou de maneira mal-intencionada, você deve revogar o acesso do usuário e reverter as alterações feitas por um adversário no seu cluster. Para obter mais informações, consulte Práticas recomendadas de segurança para o Amazon EKS no Guia do usuário do Amazon EKS.

Para obter mais informações, consulte Como corrigir as descobertas da Proteção do EKS.

DefenseEvasion:Kubernetes/TorIPCaller

Uma API comumente usada para evitar medidas defensivas foi invocada a partir de um endereço IP do nó de saída do Tor.

Gravidade padrão: alta

- Funcionalidade: logs de auditoria do EKS

Essa descoberta informa que uma operação da API foi invocada a partir de um endereço IP do nó de saída do Tor. Comumente, a API observada é associada a táticas de evasão de defesa, nas quais um adversário está tentando esconder suas ações para evitar a detecção. Tor é um software para permitir a comunicação anônima. Ele criptografa e aleatoriamente envia comunicações por meio de relés entre uma série de nós de rede. O último nó do Tor é chamado de nó de saída. Isso pode indicar um acesso não autorizado aos seu cluster do Kubernetes com a intenção de ocultar a verdadeira identidade do invasor.

Recomendações de correção:

Se o usuário relatado na descoberta na seção `KubernetesUserDetails` for `system:anonymous`, investigue por que o usuário anônimo teve permissão para invocar a API e revogue as permissões, se necessário, seguindo as instruções nas Práticas recomendadas de segurança do Amazon EKS no Guia do usuário do Amazon EKS. Se o usuário for um usuário autenticado, investigue para determinar se a atividade foi legítima ou mal-intencionada. Se a atividade for mal-intencionada, revogue o acesso do usuário e reverta as alterações feitas por um adversário no seu cluster. Para obter mais informações, consulte Como corrigir as descobertas da Proteção do EKS.

Discovery:Kubernetes/MaliciousIPCaller

Uma API comumente usada para descobrir recursos em um cluster do Kubernetes foi invocada a partir de um endereço IP.

Gravidade padrão: média

- Funcionalidade: logs de auditoria do EKS

Essa descoberta informa que uma operação de API foi invocada a partir de um endereço IP associado a atividades mal-intencionadas conhecidas. Comumente, a API observada é usada no estágio de descoberta de um ataque, no qual um invasor coleta informações para determinar se seu cluster do Kubernetes é suscetível a um ataque mais amplo.

> **Para acesso não autenticado**
>
> As descobertas MaliciousIPCaller não são geradas para acesso não autenticado. As descobertas SuccessfulAnonymousAccess não são geradas para acesso não autenticado ou anônimo.

Recomendações de correção:

Se o usuário relatado na descoberta na seção `KubernetesUserDetails` for `system:anonymous`, investigue por que o usuário anônimo teve permissão para invocar a API e revogue as permissões, se necessário, seguindo as instruções nas Práticas recomendadas de segurança do Amazon EKS no Guia do usuário do Amazon EKS. Se o usuário for um usuário autenticado, investigue para determinar se a atividade foi legítima ou mal-intencionada. Se a atividade for mal-intencionada, revogue o acesso do usuário e reverta as alterações feitas por um adversário no seu cluster. Para obter mais informações, consulte Como corrigir as descobertas da Proteção do EKS.

Discovery:Kubernetes/MaliciousIPCaller.Custom

Uma API comumente usada para descobrir recursos em um cluster do Kubernetes foi invocada a partir de um endereço IP em uma lista de ameaças personalizada.

Gravidade padrão: média

- Funcionalidade: logs de auditoria do EKS

Essa descoberta informa que uma operação da API foi invocada de um endereço IP incluído em uma lista de ameaças que você enviou. A lista de ameaças associada a essa descoberta está listada na seção Informações adicionais dos detalhes de uma descoberta. Comumente, a API observada é usada no estágio de descoberta de um ataque, no qual um invasor coleta informações para determinar se seu cluster do Kubernetes é suscetível a um ataque mais amplo.

Recomendações de correção:

Se o usuário relatado na descoberta na seção `KubernetesUserDetails` for `system:anonymous`, investigue por que o usuário anônimo teve permissão para invocar a API e revogue as permissões, se necessário, seguindo as instruções nas Práticas recomendadas de segurança do Amazon EKS no Guia do usuário do Amazon EKS. Se o usuário for um usuário autenticado, investigue para determinar se a atividade foi legítima ou mal-intencionada. Se a atividade for mal-intencionada, revogue o acesso do usuário e reverta as alterações feitas por um adversário no seu cluster. Para obter mais informações, consulte Como corrigir as descobertas da Proteção do EKS.

Discovery:Kubernetes/SuccessfulAnonymousAccess

Uma API comumente usada para descobrir recursos em um cluster do Kubernetes foi invocada por um usuário não autenticado.

Gravidade padrão: média

- Funcionalidade: logs de auditoria do EKS

Essa descoberta informa que uma operação de API foi invocada com sucesso pelo usuário `system:anonymous`. As chamadas de API feitas por `system:anonymous` não são autenticadas. Comumente, a API observada é associada ao estágio de descoberta de um ataque quando um adversário está coletando informações em seu cluster do Kubernetes. Essa atividade indica que o acesso anônimo ou não autenticado é permitido na ação da API relatada na descoberta e pode ser permitido em outras ações. Se esse comportamento não for esperado, isso pode indicar um erro de configuração ou que suas credenciais estão comprometidas.

Esse tipo de descoberta exclui os endpoints da API de verificação de integridade `/healthz`, como `/livez/readyz` e `/version`.

Recomendações de correção:

Você deve examinar as permissões que foram concedidas ao usuário `system:anonymous` em seu cluster e garantir que todas as permissões sejam necessárias. Se as permissões foram concedidas por engano ou de maneira mal-intencionada, você deve revogar o acesso do usuário e reverter as alterações feitas por um adversário no seu cluster. Para obter mais informações, consulte Práticas recomendadas de segurança para o Amazon EKS no Guia do usuário do Amazon EKS.

Para obter mais informações, consulte Como corrigir as descobertas da Proteção do EKS.

Discovery:Kubernetes/TorIPCaller

Uma API comumente usada para descobrir recursos em um cluster do Kubernetes foi invocada a partir de um endereço IP do nó de saída do Tor.

Gravidade padrão: média

- Funcionalidade: logs de auditoria do EKS

Essa descoberta informa que uma operação da API foi invocada a partir de um endereço IP do nó de saída do Tor. Comumente, a API observada é usada no estágio de descoberta de um ataque, no qual um invasor coleta informações para determinar se seu cluster do Kubernetes é suscetível a um ataque mais amplo. Tor é um software para permitir a comunicação anônima. Ele criptografa e aleatoriamente envia comunicações por meio de relés entre uma série de nós de rede. O último nó do Tor é chamado de nó de saída. Isso pode indicar um acesso não autorizado aos seu cluster do Kubernetes com a intenção de ocultar a verdadeira identidade do invasor.

Recomendações de correção:

Se o usuário relatado na descoberta na seção `KubernetesUserDetails` for `system:anonymous`, investigue por que o usuário anônimo teve permissão para invocar a API e revogue as permissões, se necessário, seguindo as instruções nas Práticas recomendadas de segurança do Amazon EKS no Guia do usuário do Amazon EKS. Se o usuário for um usuário autenticado, investigue para determinar se a atividade foi legítima ou mal-intencionada. Se a atividade for mal-intencionada, revogue o acesso do usuário e reverta as alterações feitas por um adversário no seu cluster. Para obter mais informações, consulte Como corrigir as descobertas da Proteção do EKS.

Execution:Kubernetes/ExecInKubeSystemPod

Um comando foi executado dentro de um pod dentro do namespace **`kube-system`**

Gravidade padrão: média

- Funcionalidade: logs de auditoria do EKS

Essa descoberta informa que um comando foi executado em um pod dentro do namespace `kube-system` usando a API Kubernetes exec. O namespace `kube-system` é padrão, usado principalmente para componentes de nível de sistema, como `kube-dns` e `kube-proxy`. É muito incomum executar comandos dentro de pods ou contêineres no namespace `kube-system` e pode indicar atividade suspeita.

Recomendações de correção:

Se a execução desse comando for inesperada, as credenciais da identidade do usuário usadas para executar o comando poderão ser comprometidas. Revogue o acesso do usuário e reverta todas as alterações feitas por um adversário em seu cluster. Para obter mais informações, consulte Como corrigir as descobertas da Proteção do EKS.

Impact:Kubernetes/MaliciousIPCaller

Uma API comumente usada para adulterar recursos em um cluster do Kubernetes foi invocada a partir de um endereço IP mal-intencionado conhecido.

Gravidade padrão: alta

- Funcionalidade: logs de auditoria do EKS

Essa descoberta informa que uma operação de API foi invocada a partir de um endereço IP associado a atividades mal-intencionadas conhecidas. A API observada é comumente associada a táticas de impacto em que um adversário está tentando manipular, interromper ou destruir dados em seu ambiente. AWS

Recomendações de correção:

Se o usuário relatado na descoberta na seção `KubernetesUserDetails` for `system:anonymous`, investigue por que o usuário anônimo teve permissão para invocar a API e revogue as permissões,

se necessário, seguindo as instruções nas Práticas recomendadas de segurança do Amazon EKS no Guia do usuário do Amazon EKS. Se o usuário for um usuário autenticado, investigue para determinar se a atividade foi legítima ou mal-intencionada. Se a atividade for mal-intencionada, revogue o acesso do usuário e reverta as alterações feitas por um adversário no seu cluster. Para obter mais informações, consulte Como corrigir as descobertas da Proteção do EKS.

Impact:Kubernetes/MaliciousIPCaller.Custom

Uma API comumente usada para adulterar recursos em um cluster do Kubernetes foi invocada a partir de um endereço IP em uma lista de ameaças personalizada.

Gravidade padrão: alta

- Funcionalidade: logs de auditoria do EKS

Essa descoberta informa que uma operação de API foi invocada a partir de um endereço IP incluído em uma lista de ameaças que você carregou. A lista de ameaças associada a essa descoberta está listada na seção Informações adicionais dos detalhes de uma descoberta. A API observada é comumente associada a táticas de impacto em que um adversário está tentando manipular, interromper ou destruir dados em seu ambiente. AWS

Recomendações de correção:

Se o usuário relatado na descoberta na seção `KubernetesUserDetails` for `system:anonymous`, investigue por que o usuário anônimo teve permissão para invocar a API e revogue as permissões, se necessário, seguindo as instruções nas Práticas recomendadas de segurança do Amazon EKS no Guia do usuário do Amazon EKS. Se o usuário for um usuário autenticado, investigue para determinar se a atividade foi legítima ou mal-intencionada. Se a atividade for mal-intencionada, revogue o acesso do usuário e reverta as alterações feitas por um adversário no seu cluster. Para obter mais informações, consulte Como corrigir as descobertas da Proteção do EKS.

Impact:Kubernetes/SuccessfulAnonymousAccess

Uma API comumente usada para adulterar recursos em um cluster do Kubernetes foi invocada por um usuário não autenticado.

Gravidade padrão: alta

- Funcionalidade: logs de auditoria do EKS

Essa descoberta informa que uma operação de API foi invocada com sucesso pelo usuário `system:anonymous`. As chamadas de API feitas por `system:anonymous` não são autenticadas. Comumente, a API observada é associada ao estágio de impacto de um ataque quando um adversário está adulterando recursos em seu cluster. Essa atividade indica que o acesso anônimo ou não autenticado é permitido na ação da API relatada na descoberta e pode ser permitido em outras ações. Se esse comportamento não for esperado, isso pode indicar um erro de configuração ou que suas credenciais estão comprometidas.

Recomendações de correção:

Você deve examinar as permissões que foram concedidas ao usuário `system:anonymous` em seu cluster e garantir que todas as permissões sejam necessárias. Se as permissões foram concedidas por engano ou de maneira mal-intencionada, você deve revogar o acesso do usuário e reverter as alterações feitas por um adversário no seu cluster. Para obter mais informações, consulte Práticas recomendadas de segurança para o Amazon EKS no Guia do usuário do Amazon EKS.

Para obter mais informações, consulte Como corrigir as descobertas da Proteção do EKS.

Impact:Kubernetes/TorIPCaller

Uma API comumente usada para adulterar recursos em um cluster do Kubernetes foi invocada a partir de um endereço IP do nó de saída do Tor.

Gravidade padrão: alta

- Funcionalidade: logs de auditoria do EKS

Essa descoberta informa que uma operação da API foi invocada a partir de um endereço IP do nó de saída do Tor. Comumente, a API observada é associada a táticas de impacto em que um adversário está tentando manipular, interromper ou destruir dados em seu ambiente da AWS . Tor é um software para permitir a comunicação anônima. Ele criptografa e aleatoriamente envia comunicações por meio de relés entre uma série de nós de rede. O último nó do Tor é chamado de nó de saída. Isso pode indicar um acesso não autorizado aos seu cluster do Kubernetes com a intenção de ocultar a verdadeira identidade do invasor.

Recomendações de correção:

Se o usuário relatado na descoberta na seção `KubernetesUserDetails` for `system:anonymous`, investigue por que o usuário anônimo teve permissão para invocar a API e revogue as permissões,

se necessário, seguindo as instruções nas Práticas recomendadas de segurança do Amazon EKS no Guia do usuário do Amazon EKS. Se o usuário for um usuário autenticado, investigue para determinar se a atividade foi legítima ou mal-intencionada. Se a atividade for mal-intencionada, revogue o acesso do usuário e reverta as alterações feitas por um adversário no seu cluster. Para obter mais informações, consulte Como corrigir as descobertas da Proteção do EKS.

Persistence:Kubernetes/MaliciousIPCaller

Uma API comumente usada para obter acesso persistente a um cluster do Kubernetes foi invocada a partir de um endereço IP mal-intencionado conhecido.

Gravidade padrão: média

- Funcionalidade: logs de auditoria do EKS

Essa descoberta informa que uma operação de API foi invocada a partir de um endereço IP associado a atividades mal-intencionadas conhecidas. Comumente, a API observada é associada a táticas de persistência em que um adversário obteve acesso ao seu cluster do Kubernetes e está tentando manter esse acesso.

Recomendações de correção:

Se o usuário relatado na descoberta na seção `KubernetesUserDetails` for `system:anonymous`, investigue por que o usuário anônimo teve permissão para invocar a API e revogue as permissões, se necessário, seguindo as instruções nas Práticas recomendadas de segurança do Amazon EKS no Guia do usuário do Amazon EKS. Se o usuário for um usuário autenticado, investigue para determinar se a atividade foi legítima ou mal-intencionada. Se a atividade for mal-intencionada, revogue o acesso do usuário e reverta as alterações feitas por um adversário no seu cluster. Para obter mais informações, consulte Como corrigir as descobertas da Proteção do EKS.

Persistence:Kubernetes/MaliciousIPCaller.Custom

Uma API comumente usada para obter acesso persistente a um cluster do Kubernetes foi invocada a partir de um endereço IP em uma lista de ameaças personalizada.

Gravidade padrão: média

- Funcionalidade: logs de auditoria do EKS

Essa descoberta informa que uma operação de API foi invocada a partir de um endereço IP incluído em uma lista de ameaças que você carregou. A lista de ameaças associada a essa descoberta está listada na seção Informações adicionais dos detalhes de uma descoberta. Comumente, a API observada é associada a táticas de persistência em que um adversário obteve acesso ao seu cluster do Kubernetes e está tentando manter esse acesso.

Recomendações de correção:

Se o usuário relatado na descoberta na seção `KubernetesUserDetails` for `system:anonymous`, investigue por que o usuário anônimo teve permissão para invocar a API e revogue as permissões, se necessário, seguindo as instruções nas Práticas recomendadas de segurança do Amazon EKS no Guia do usuário do Amazon EKS. Se o usuário for um usuário autenticado, investigue para determinar se a atividade foi legítima ou mal-intencionada. Se a atividade for mal-intencionada, revogue o acesso do usuário e reverta as alterações feitas por um adversário no seu cluster. Para obter mais informações, consulte Como corrigir as descobertas da Proteção do EKS.

Persistence:Kubernetes/SuccessfulAnonymousAccess

Uma API comumente usada para obter permissões de alto nível para um cluster do Kubernetes foi invocada por um usuário não autenticado.

Gravidade padrão: alta

- Funcionalidade: logs de auditoria do EKS

Essa descoberta informa que uma operação de API foi invocada com sucesso pelo usuário `system:anonymous`. As chamadas de API feitas por `system:anonymous` não são autenticadas. Comumente, a API observada é associada às táticas de persistência em que um adversário obteve acesso ao seu cluster e está tentando manter esse acesso. Essa atividade indica que o acesso anônimo ou não autenticado é permitido na ação da API relatada na descoberta e pode ser permitido em outras ações. Se esse comportamento não for esperado, isso pode indicar um erro de configuração ou que suas credenciais estão comprometidas.

Recomendações de correção:

Você deve examinar as permissões que foram concedidas ao usuário `system:anonymous` em seu cluster e garantir que todas as permissões sejam necessárias. Se as permissões foram concedidas por engano ou de maneira mal-intencionada, você deve revogar o acesso do usuário e reverter as

alterações feitas por um adversário no seu cluster. Para obter mais informações, consulte Práticas recomendadas de segurança para o Amazon EKS no Guia do usuário do Amazon EKS.

Para obter mais informações, consulte Como corrigir as descobertas da Proteção do EKS.

Persistence:Kubernetes/TorIPCaller

Uma API comumente usada para obter acesso persistente a um cluster do Kubernetes foi invocada a partir de um endereço IP do nó de saída do Tor.

Gravidade padrão: média

- Funcionalidade: logs de auditoria do EKS

Essa descoberta informa que uma operação da API foi invocada a partir de um endereço IP do nó de saída do Tor. Comumente, a API observada é associada a táticas de persistência em que um adversário obteve acesso ao seu cluster do Kubernetes e está tentando manter esse acesso. Tor é um software para permitir a comunicação anônima. Ele criptografa e aleatoriamente envia comunicações por meio de relés entre uma série de nós de rede. O último nó do Tor é chamado de nó de saída. Isso pode indicar acesso não autorizado aos seus AWS recursos com a intenção de ocultar a verdadeira identidade do atacante.

Recomendações de correção:

Se o usuário relatado na descoberta na seção `KubernetesUserDetails` for `system:anonymous`, investigue por que o usuário anônimo teve permissão para invocar a API e revogue as permissões, se necessário, seguindo as instruções nas Práticas recomendadas de segurança do Amazon EKS no Guia do usuário do Amazon EKS. Se o usuário for um usuário autenticado, investigue para determinar se a atividade foi legítima ou mal-intencionada. Se a atividade for mal-intencionada, revogue o acesso do usuário e reverta as alterações feitas por um adversário no seu cluster. Para obter mais informações, consulte Como corrigir as descobertas da Proteção do EKS.

Policy:Kubernetes/AdminAccessToDefaultServiceAccount

A conta de serviço padrão recebeu privilégios de administrador em um cluster do Kubernetes.

Gravidade padrão: alta

- Funcionalidade: logs de auditoria do EKS

Essa descoberta informa que a conta de serviço padrão de um namespace em seu cluster do Kubernetes recebeu privilégios de administrador. O Kubernetes cria uma conta de serviço padrão para todos os namespaces no cluster. Ele atribui automaticamente a conta de serviço padrão como uma identidade aos pods que não foram explicitamente associados a outra conta de serviço. Se a conta de serviço padrão tiver privilégios de administrador, isso poderá resultar no lançamento involuntário de pods com privilégios de administrador. Se esse comportamento não for esperado, isso pode indicar um erro de configuração ou que suas credenciais estão comprometidas.

Recomendações de correção:

Não use a conta de serviço padrão para conceder permissões aos pods. Em vez disso, você deve criar uma conta de serviço dedicada para cada workload e conceder permissão a essa conta de acordo com as necessidades. Para corrigir esse problema, você deve criar contas de serviço dedicadas para todos os seus pods e workloads e atualizar os pods e workloads para migrar da conta de serviço padrão para suas contas dedicadas. Em seguida, é necessário remover a permissão de administrador da conta de serviço padrão. Para obter mais informações, consulte Como corrigir as descobertas da Proteção do EKS.

Policy:Kubernetes/AnonymousAccessGranted

O usuário **`system:anonymous`** recebeu permissão de API em um cluster Kubernetes.

Gravidade padrão: alta

- Funcionalidade: logs de auditoria do EKS

Essa descoberta informa que um usuário em seu cluster do Kubernetes criou com sucesso um `ClusterRoleBinding` ou `RoleBinding` para vincular o usuário `system:anonymous` a um perfil. Isso permite acesso não autenticado às operações de API permitidas pelo perfil. Se esse comportamento não for esperado, isso pode indicar um erro de configuração ou que suas credenciais estão comprometidas

Recomendações de correção:

Você deve examinar as permissões que foram concedidas ao usuário `system:anonymous` ou grupo `system:unauthenticated` em seu cluster e revogar o acesso anônimo desnecessário. Para obter mais informações, consulte Práticas recomendadas de segurança para o Amazon EKS no Guia do

usuário do Amazon EKS. Se as permissões foram concedidas de maneira mal-intencionada, você deve revogar o acesso do usuário que concedeu as permissões e reverter quaisquer alterações feitas por um adversário em seu cluster. Para obter mais informações, consulte Como corrigir as descobertas da Proteção do EKS.

Policy:Kubernetes/ExposedDashboard

O painel de um cluster do Kubernetes foi exposto à Internet

Gravidade padrão: média

- Funcionalidade: logs de auditoria do EKS

Essa descoberta informa que o painel do Kubernetes do seu cluster foi exposto à Internet por um serviço de balanceador de carga. Um painel exposto torna a interface de gerenciamento do seu cluster acessível pela Internet e permite que os adversários explorem quaisquer lacunas de autenticação e controle de acesso que possam estar presentes.

Recomendações de correção:

Você deve garantir que a autenticação e a autorização fortes sejam aplicadas no Painel do Kubernetes. Você também deve implementar o controle de acesso à rede para restringir o acesso ao painel a partir de endereços IP específicos.

Para obter mais informações, consulte Como corrigir as descobertas da Proteção do EKS.

Policy:Kubernetes/KubeflowDashboardExposed

A ferramenta Kubeflow o painel de um cluster Kubernetes foi exposto à Internet

Gravidade padrão: média

- Funcionalidade: logs de auditoria do EKS

Essa descoberta informa que o painel Kubeflow do seu cluster foi exposto à Internet por um serviço de balanceador de carga. Um painel exposto do Kubeflow torna a interface de gerenciamento do seu ambiente Kubeflow acessível pela Internet e permite que os adversários explorem quaisquer lacunas de autenticação e controle de acesso que possam estar presentes.

Recomendações de correção:

Você deve garantir que a autenticação e a autorização fortes sejam aplicadas no Painel Kubeflow. Você também deve implementar o controle de acesso à rede para restringir o acesso ao painel a partir de endereços IP específicos.

Para obter mais informações, consulte Como corrigir as descobertas da Proteção do EKS.

CredentialAccess:Kubernetes/AnomalousBehavior.SecretsAccessed

Uma API do Kubernetes comumente usada para acessar segredos foi invocada de forma anômala.

Gravidade padrão: média

- Funcionalidade: logs de auditoria do EKS

Essa descoberta informa que uma operação anômala de API para recuperar segredos confidenciais do cluster foi invocada por um usuário do Kubernetes em seu cluster. Comumente, a API observada é associada a táticas de acesso a credenciais que podem levar a um escalonamento privilegiado e a um maior acesso ao seu cluster. Se esse comportamento não for esperado, isso pode indicar um erro de configuração ou que suas credenciais da AWS estão comprometidas.

A API observada foi identificada como anômala pelo modelo de aprendizado de máquina (ML) de detecção de GuardDuty anomalias. O modelo de ML avalia todas as atividades da API do usuário em seu cluster do EKS e identifica eventos anômalos associados a técnicas usadas por usuários não autorizados. O modelo de ML rastreia vários fatores da operação da API, como o usuário que fez a solicitação, o local de onde a solicitação foi feita, o agente do usuário usado e o namespace que o usuário operou. Você pode encontrar os detalhes incomuns da solicitação de API no painel de busca de detalhes no GuardDuty console.

Recomendações de correção:

Examine as permissões concedidas ao usuário do Kubernetes em seu cluster e garanta que todas essas permissões sejam necessárias. Se as permissões foram concedidas por engano ou de maneira mal-intencionada, revogue o acesso do usuário e reverta as alterações feitas por um usuário não autorizado em seu cluster. Para obter mais informações, consulte Como corrigir as descobertas da Proteção do EKS.

Se suas AWS credenciais estiverem comprometidas, consulte. Correção de problemas potencialmente comprometidos AWS credenciais

PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleBindingCreated

Um RoleBinding ou ClusterRoleBinding para um papel excessivamente permissivo ou namespace confidencial foi criado ou modificado em seu cluster Kubernetes.

Gravidade padrão: média*

> **Note**
>
> A gravidade padrão desta descoberta é Média. No entanto, se um RoleBinding ou ClusterRoleBinding envolver o ClusterRoles `admin` ou`cluster-admin`, a gravidade será Alta.

- Funcionalidade: logs de auditoria do EKS

Essa descoberta informa que um usuário em seu cluster do Kubernetes criou um `RoleBinding` ou `ClusterRoleBinding` para vincular um usuário a uma função com permissões de administrador ou namespaces confidenciais. Se esse comportamento não for esperado, isso pode indicar um erro de configuração ou que suas credenciais da AWS estão comprometidas.

A API observada foi identificada como anômala pelo modelo de aprendizado de máquina (ML) de detecção de GuardDuty anomalias. O modelo de ML avalia todas as atividades da API do usuário em seu cluster do EKS. Esse modelo de ML também identifica eventos anômalos associados às técnicas usadas por um usuário não autorizado. O modelo de ML também rastreia vários fatores da operação da API, como o usuário que fez a solicitação, o local de onde a solicitação foi feita, o agente do usuário usado e o namespace que o usuário operou. Você pode encontrar os detalhes incomuns da solicitação de API no painel de busca de detalhes no GuardDuty console.

Recomendações de correção:

Examine as permissões concedidas ao usuário do Kubernetes. Essas permissões são definidas na função e nos assuntos envolvidos em `RoleBinding` e `ClusterRoleBinding`. Se as permissões foram concedidas por engano ou de maneira mal-intencionada, revogue o acesso do usuário e reverta as alterações feitas por um usuário não autorizado em seu cluster. Para obter mais informações, consulte Como corrigir as descobertas da Proteção do EKS.

Se suas AWS credenciais estiverem comprometidas, consulte. Correção de problemas potencialmente comprometidos AWS credenciais

Execution:Kubernetes/AnomalousBehavior.ExecInPod

Um comando foi executado dentro de um pod de forma anômala.

Gravidade padrão: média

- Funcionalidade: logs de auditoria do EKS

Essa descoberta informa que um comando foi executado em um pod usando a API Kubernetes exec. A API Kubernetes exec permite executar comandos arbitrários em um pod. Se esse comportamento não for esperado para o usuário, namespace ou pod, isso pode indicar um erro de configuração ou que suas AWS credenciais estão comprometidas.

A API observada foi identificada como anômala pelo modelo de aprendizado de máquina (ML) de detecção de GuardDuty anomalias. O modelo de ML avalia todas as atividades da API do usuário em seu cluster do EKS. Esse modelo de ML também identifica eventos anômalos associados às técnicas usadas por um usuário não autorizado. O modelo de ML também rastreia vários fatores da operação da API, como o usuário que fez a solicitação, o local de onde a solicitação foi feita, o agente do usuário usado e o namespace que o usuário operou. Você pode encontrar os detalhes incomuns da solicitação de API no painel de busca de detalhes no GuardDuty console.

Recomendações de correção:

Se a execução desse comando for inesperada, as credenciais da identidade do usuário usadas para executar o comando podem ter sido comprometidas. Revogue o acesso do usuário e reverta todas as alterações feitas por um usuário não autorizado em seu cluster. Para obter mais informações, consulte Como corrigir as descobertas da Proteção do EKS.

Se suas AWS credenciais estiverem comprometidas, consulte. Correção de problemas potencialmente comprometidos AWS credenciais

PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!PrivilegedContainer

Uma workload foi lançada com um contêiner privilegiado de forma anômala.

Gravidade padrão: alta

- Funcionalidade: logs de auditoria do EKS

Essa descoberta informa que uma workload foi lançada com um contêiner privilegiado em seu cluster Amazon EKS. Um contêiner privilegiado tem acesso de nível raiz ao host. Usuários não autorizados podem lançar contêineres privilegiados como uma tática de escalonamento de privilégios para primeiro obter acesso ao host e depois comprometê-lo.

A criação ou modificação observada do contêiner foi identificada como anômala pelo modelo de aprendizado de máquina (ML) de detecção de GuardDuty anomalias. O modelo de ML avalia todas as atividades da API do usuário e da imagem do contêiner em seu cluster do EKS. Esse modelo de ML também identifica eventos anômalos associados às técnicas usadas por um usuário não autorizado. O modelo de ML também rastreia vários fatores da operação da API, como o usuário que fez a solicitação, o local de onde a solicitação foi feita, o agente do usuário usado, as imagens de contêiner observadas em sua conta e o namespace operado pelo usuário. Você pode encontrar os detalhes incomuns da solicitação de API no painel de busca de detalhes no GuardDuty console.

Recomendações de correção:

Se o lançamento desse contêiner for inesperado, as credenciais da identidade do usuário usadas para iniciar o contêiner podem ter sido comprometidas. Revogue o acesso do usuário e reverta todas as alterações feitas por um usuário não autorizado em seu cluster. Para obter mais informações, consulte Como corrigir as descobertas da Proteção do EKS.

Se suas AWS credenciais estiverem comprometidas, consulte. Correção de problemas potencialmente comprometidos AWS credenciais

Se o lançamento desse contêiner for esperado, é recomendável usar uma regra de supressão com um critério de filtro baseado no campo `resource.KubernetesDetails.KubernetesWorkloadDetails.containers.imagePrefix`. Nos critérios de filtro, o campo `imagePrefix` deve ter o mesmo valor do campo `imagePrefix` especificado na descoberta. Para obter mais informações, consulte Regras de supressão em GuardDuty.

Persistence:Kubernetes/AnomalousBehavior.WorkloadDeployed! ContainerWithSensitiveMount

Uma workload foi implantada de forma anômala, com um caminho de host sensível montado dentro da workload.

Gravidade padrão: alta

- Funcionalidade: logs de auditoria do EKS

Essa descoberta informa que uma workload foi lançada com um contêiner que incluía um caminho de host confidencial na seção `volumeMounts`. Isso potencialmente torna o caminho confidencial do host acessível e gravável de dentro do contêiner. Essa técnica é comumente usada por usuários não autorizados para obter acesso ao sistema de arquivos do host.

A criação ou modificação observada do contêiner foi identificada como anômala pelo modelo de aprendizado de máquina (ML) de detecção de GuardDuty anomalias. O modelo de ML avalia todas as atividades da API do usuário e da imagem do contêiner em seu cluster do EKS. Esse modelo de ML também identifica eventos anômalos associados às técnicas usadas por um usuário não autorizado. O modelo de ML também rastreia vários fatores da operação da API, como o usuário que fez a solicitação, o local de onde a solicitação foi feita, o agente do usuário usado, as imagens de contêiner observadas em sua conta e o namespace operado pelo usuário. Você pode encontrar os detalhes incomuns da solicitação de API no painel de busca de detalhes no GuardDuty console.

Recomendações de correção:

Se o lançamento desse contêiner for inesperado, as credenciais da identidade do usuário usadas para iniciar o contêiner podem ter sido comprometidas. Revogue o acesso do usuário e reverta todas as alterações feitas por um usuário não autorizado em seu cluster. Para obter mais informações, consulte Como corrigir as descobertas da Proteção do EKS.

Se suas AWS credenciais estiverem comprometidas, consulte. Correção de problemas potencialmente comprometidos AWS credenciais

Se o lançamento desse contêiner for esperado, é recomendável usar uma regra de supressão com um critério de filtro baseado no campo `resource.KubernetesDetails.KubernetesWorkloadDetails.containers.imagePrefix`. Nos critérios de filtro, o campo `imagePrefix` deve ter o mesmo valor do campo `imagePrefix` especificado na descoberta. Para obter mais informações, consulte Regras de supressão em GuardDuty.

Execution:Kubernetes/AnomalousBehavior.WorkloadDeployed

Uma workload foi lançada de forma anômala.

Gravidade padrão: baixa*

> **Note**
>
> A gravidade padrão é Baixa. No entanto, se a workload contiver um nome de imagem potencialmente suspeito, como uma ferramenta de teste de penetração conhecida, ou um contêiner executando um comando potencialmente suspeito na inicialização, como comandos de shell reverso, a gravidade desse tipo de descoberta será considerada Média.

- Funcionalidade: logs de auditoria do EKS

Essa descoberta informa que uma workload do Kubernetes foi criada ou modificada de forma anômala, como uma atividade de API, novas imagens de contêiner ou configuração de workload arriscada, dentro do seu cluster Amazon EKS. Usuários não autorizados podem lançar contêineres como uma tática para executar código arbitrário para primeiro obter acesso ao host e depois comprometê-lo.

A criação ou modificação observada do contêiner foi identificada como anômala pelo modelo de aprendizado de máquina (ML) de detecção de GuardDuty anomalias. O modelo de ML avalia todas as atividades da API do usuário e da imagem do contêiner em seu cluster do EKS. Esse modelo de ML também identifica eventos anômalos associados às técnicas usadas por um usuário não autorizado. O modelo de ML também rastreia vários fatores da operação da API, como o usuário que fez a solicitação, o local de onde a solicitação foi feita, o agente do usuário usado, as imagens de contêiner observadas em sua conta e o namespace operado pelo usuário. Você pode encontrar os detalhes incomuns da solicitação de API no painel de busca de detalhes no GuardDuty console.

Recomendações de correção:

Se o lançamento desse contêiner for inesperado, as credenciais da identidade do usuário usadas para iniciar o contêiner podem ter sido comprometidas. Revogue o acesso do usuário e reverta todas as alterações feitas por um usuário não autorizado em seu cluster. Para obter mais informações, consulte Como corrigir as descobertas da Proteção do EKS.

Se suas AWS credenciais estiverem comprometidas, consulte. Correção de problemas potencialmente comprometidos AWS credenciais

Se o lançamento desse contêiner for esperado, é recomendável usar uma regra de supressão com um critério de filtro baseado no campo `resource.KubernetesDetails.KubernetesWorkloadDetails.containers.imagePrefix`. Nos critérios de filtro, o campo `imagePrefix` deve ter o mesmo valor do campo `imagePrefix`

especificado na descoberta. Para obter mais informações, consulte Regras de supressão em GuardDuty.

PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleCreated

Uma função altamente permissiva ou ClusterRole foi criada ou modificada de forma anômala.

Gravidade padrão: baixa

- Funcionalidade: logs de auditoria do EKS

Essa descoberta informa que uma operação de API anômala para criar `Role` ou `ClusterRole` com permissões excessivas foi chamada por um usuário do Kubernetes em seu cluster Amazon EKS. Os atores podem usar a criação de funções com permissões poderosas para evitar o uso de funções internas semelhantes às de administrador e evitar a detecção. As permissões excessivas podem levar a escalonamento privilegiado, execução remota de código e, potencialmente, controle sobre um namespace ou cluster. Se esse comportamento não for esperado, isso pode indicar um erro de configuração ou que suas credenciais estão comprometidas.

A API observada foi identificada como anômala pelo modelo de aprendizado de máquina (ML) de detecção de GuardDuty anomalias. O modelo de ML avalia todas as atividades de API do usuário em seu cluster Amazon EKS e identifica eventos anômalos associados às técnicas usadas por usuários não autorizados. O modelo de ML também rastreia vários fatores da operação da API, como o usuário que fez a solicitação, o local de onde a solicitação foi feita, o agente do usuário usado, as imagens de contêiner observadas em sua conta e o namespace operado pelo usuário. Você pode encontrar os detalhes incomuns da solicitação de API no painel de busca de detalhes no GuardDuty console.

Recomendações de correção:

Examine as permissões definidas em `Role` ou `ClusterRole` para garantir que todas as permissões sejam necessárias e siga os princípios de privilégios mínimos. Se as permissões foram concedidas por engano ou de maneira mal-intencionada, revogue o acesso do usuário e reverta as alterações feitas por um usuário não autorizado em seu cluster. Para obter mais informações, consulte Como corrigir as descobertas da Proteção do EKS.

Se suas AWS credenciais estiverem comprometidas, consulte. Correção de problemas potencialmente comprometidos AWS credenciais

Discovery:Kubernetes/AnomalousBehavior.PermissionChecked

Um usuário verificou sua permissão de acesso de forma anômala.

Gravidade padrão: baixa

- Funcionalidade: logs de auditoria do EKS

Essa descoberta informa que um usuário em seu cluster do Kubernetes verificou com sucesso se as poderosas permissões conhecidas que podem levar ao escalonamento privilegiado e à execução remota de código são permitidas. Por exemplo, um comando comum usado para verificar as permissões de um usuário é `kubectl auth can-i`. Se esse comportamento não for esperado, isso pode indicar um erro de configuração ou que suas credenciais foram comprometidas.

A API observada foi identificada como anômala pelo modelo de aprendizado de máquina (ML) de detecção de GuardDuty anomalias. O modelo de ML avalia todas as atividades de API do usuário em seu cluster Amazon EKS e identifica eventos anômalos associados às técnicas usadas por usuários não autorizados. O modelo de ML também rastreia vários fatores da operação da API, como o usuário que fez a solicitação, o local de onde a solicitação foi feita, a permissão que está sendo verificada e o namespace que o usuário operou. Você pode encontrar os detalhes incomuns da solicitação de API no painel de busca de detalhes no GuardDuty console.

Recomendações de correção:

Examine as permissões concedidas ao usuário do Kubernetes para garantir que todas as permissões sejam necessárias. Se as permissões foram concedidas por engano ou de maneira mal-intencionada, revogue o acesso do usuário e reverta as alterações feitas por um usuário não autorizado em seu cluster. Para obter mais informações, consulte Como corrigir as descobertas da Proteção do EKS.

Se suas AWS credenciais estiverem comprometidas, consulte. Correção de problemas potencialmente comprometidos AWS credenciais

GuardDuty Tipos de descoberta de monitoramento de tempo de execução

A Amazon GuardDuty gera as seguintes descobertas do Runtime Monitoring para indicar possíveis ameaças com base no comportamento em nível de sistema operacional dos hosts e contêineres do

Amazon EC2 em seus clusters do Amazon EKS, cargas de trabalho do Fargate e do Amazon ECS e instâncias do Amazon EC2.

GuardDuty gera alguns tipos de descoberta do Runtime Monitoring somente quando você ativa as Regras de Detecção Personalizadas para o Runtime Monitoring. Para esses tipos de descoberta, consulteEncontrando tipos que exigem regras de detecção personalizadas.

> **Note**
>
> Os tipos de descoberta do Monitoramento de runtime são baseados nos logs de runtime coletados dos hosts. Os registros contêm campos, como caminhos de arquivos, que podem ser controlados por um agente mal-intencionado. Esses campos também estão incluídos nas GuardDuty descobertas para fornecer contexto de tempo de execução. Ao processar as descobertas do Runtime Monitoring fora do GuardDuty console, você deve higienizar os campos de busca. Por exemplo, é possível codificar em HTML os campos de busca ao exibi-los em uma página da Web.

Tópicos

- Encontrando tipos que o Runtime Monitoring gera por padrão
- Encontrando tipos que exigem regras de detecção personalizadas

Encontrando tipos que o Runtime Monitoring gera por padrão

GuardDuty gera os tipos de descoberta nesta seção quando você ativa o Runtime Monitoring. Você não precisa ativar as Regras de Detecção Personalizadas para o Runtime Monitoring para obter esses tipos de descoberta.

Tópicos

- CryptoCurrency:Runtime/BitcoinTool.B
- Backdoor:Runtime/C&CActivity.B
- UnauthorizedAccess:Runtime/TorRelay
- UnauthorizedAccess:Runtime/TorClient
- Trojan:Runtime/BlackholeTraffic
- Trojan:Runtime/DropPoint
- CryptoCurrency:Runtime/BitcoinTool.B! DNS

- Backdoor:Runtime/C&CActivity.B! DNS
- Trojan:Runtime/BlackholeTraffic! DNS
- Trojan:Runtime/DropPoint! DNS
- Trojan:Runtime/DGADomainRequest.C! DNS
- Trojan:Runtime/DriveBySourceTraffic! DNS
- Trojan:Runtime/PhishingDomainRequest! DNS
- Impact:Runtime/AbusedDomainRequest.Reputation
- Impact:Runtime/BitcoinDomainRequest.Reputation
- Impact:Runtime/MaliciousDomainRequest.Reputation
- Impact:Runtime/SuspiciousDomainRequest.Reputation
- UnauthorizedAccess:Runtime/MetadataDNSRebind
- Execution:Runtime/NewBinaryExecuted
- PrivilegeEscalation:Runtime/DockerSocketAccessed
- PrivilegeEscalation:Runtime/RuncContainerEscape
- PrivilegeEscalation:Runtime/CGroupsReleaseAgentModified
- DefenseEvasion:Runtime/ProcessInjection.Proc
- DefenseEvasion:Runtime/ProcessInjection.Ptrace
- DefenseEvasion:Runtime/ProcessInjection.VirtualMemoryWrite
- Execution:Runtime/ReverseShell
- DefenseEvasion:Runtime/FilelessExecution
- Impact:Runtime/CryptoMinerExecuted
- Execution:Runtime/NewLibraryLoaded
- PrivilegeEscalation:Runtime/ContainerMountsHostDirectory
- PrivilegeEscalation:Runtime/UserfaultfdUsage
- Execution:Runtime/SuspiciousTool
- Execution:Runtime/SuspiciousCommand
- DefenseEvasion:Runtime/SuspiciousCommand
- DefenseEvasion:Runtime/PtraceAntiDebugging
- Execution:Runtime/MaliciousFileExecuted
- Execution:Runtime/MaliciousFileExecuted.Custom

- Execution:Runtime/SuspiciousShellCreated
- PrivilegeEscalation:Runtime/ElevationToRoot
- Discovery:Runtime/SuspiciousCommand
- Persistence:Runtime/SuspiciousCommand
- PrivilegeEscalation:Runtime/SuspiciousCommand
- DefenseEvasion:Runtime/KernelModuleLoaded
- Persistence:Runtime/SensitiveFileModified
- PrivilegeEscalation:Runtime/SensitiveFileModified
- DefenseEvasion:Runtime/SensitiveFileModified

CryptoCurrency:Runtime/BitcoinTool.B

Uma instância do Amazon EC2 ou um contêiner está consultando um endereço IP associado à atividade relacionada à criptomoeda.

Gravidade padrão: alta

- Atributo: Monitoramento de runtime

Essa descoberta informa que um processo em execução na instância do EC2 listada ou um contêiner em seu ambiente da AWS está consultando um endereço IP associado a uma atividade relacionada a criptomoedas. Os agentes de ameaças podem tentar assumir o controle dos recursos computacionais para redirecioná-los de maneira mal-intencionada para a mineração não autorizada de criptomoedas.

O agente GuardDuty de tempo de execução monitora eventos de vários tipos de recursos. Para identificar o recurso potencialmente comprometido, visualize o tipo de recurso no painel de descobertas no GuardDuty console. Está disponível contexto adicional, incluindo informações sobre o processo e a linhagem do processo, na descoberta para uma investigação mais aprofundada.

Recomendações de correção:

Se você usar essa instância do EC2 ou um contêiner para minerar ou gerenciar criptomoeda, ou se essa instância ou contêiner estiverem envolvidos de outra forma na atividade de blockchain, a descoberta CryptoCurrency:Runtime/BitcoinTool.B poderia representar uma atividade esperada para o ambiente. Se esse for o caso em seu AWS ambiente, recomendamos que você configure

uma regra de supressão para essa descoberta. A regra de supressão deve consistir em dois critérios de filtro. O primeiro critério deve usar o atributo Tipo de descoberta com um valor de `CryptoCurrency:Runtime/BitcoinTool.B`. O segundo critério de filtro deve ser o ID da instância ou o ID da imagem do contêiner envolvido na atividade relacionada à criptomoeda ou blockchain. Para obter mais informações, consulte Regras de supressão.

Se essa atividade for inesperada, seu recurso pode estar comprometido. Para obter mais informações, consulte Como corrigir as descobertas do Monitoramento de runtime.

Backdoor:Runtime/C&CActivity.B

Uma instância do Amazon EC2 ou um contêiner está consultando um nome de domínio associado a um servidor de comando e controle conhecido.

Gravidade padrão: alta

- Atributo: Monitoramento de runtime

Essa descoberta informa que um processo em execução na instância do EC2 listada ou um contêiner em seu ambiente da AWS está consultando um endereço IP associado a um servidor de comando e controle (C&C) conhecido. A instância ou o contêiner listado podem estar potencialmente comprometidos. Os servidores de comando e controle são computadores que enviam comandos para membros de um botnet.

Um botnet é uma coleção de dispositivos conectados à Internet (que podem incluir PCs, servidores, dispositivos móveis e dispositivos de Internet das Coisas) infectados e controlados por um tipo comum de malware. Os botnets são frequentemente usados para distribuir malwares e coletar informações inapropriadas, como números de cartão de crédito. Dependendo da finalidade e da estrutura do botnet, o servidor de C&C também pode emitir comandos para iniciar um ataque de negação de serviço distribuída (DDoS).

> **Note**
>
> Se o IP consultado estiver relacionado ao log4j, os campos da descoberta associada incluirão os seguintes valores:
>
> - `service.additionalInfo.threatListName = Amazon`
> - `service.additionalInfo.threatName = Log4j Related`

O agente GuardDuty de tempo de execução monitora eventos de vários tipos de recursos. Para identificar o recurso potencialmente comprometido, visualize o tipo de recurso no painel de descobertas no GuardDuty console. Está disponível contexto adicional, incluindo informações sobre o processo e a linhagem do processo, na descoberta para uma investigação mais aprofundada.

Recomendações de correção:

Se essa atividade for inesperada, seu recurso pode estar comprometido. Para obter mais informações, consulte Como corrigir as descobertas do Monitoramento de runtime.

UnauthorizedAccess:Runtime/TorRelay

Sua instância do Amazon EC2 ou um contêiner está fazendo conexões com uma rede Tor como uma retransmissão Tor.

Gravidade padrão: alta

- Atributo: Monitoramento de runtime

Essa descoberta informa que um processo em execução na instância EC2 listada ou em um contêiner em seu AWS ambiente está fazendo conexões com uma rede Tor de uma maneira que sugere que ela está agindo como um retransmissor Tor. Tor é um software para permitir a comunicação anônima. Retransmissões Tor aumentam o anonimato da comunicação encaminhando o tráfego possivelmente ilícito do cliente de uma retransmissão Tor para outra.

O agente GuardDuty de tempo de execução monitora eventos de vários tipos de recursos. Para identificar o recurso potencialmente comprometido, visualize o tipo de recurso no painel de descobertas no GuardDuty console. Está disponível contexto adicional, incluindo informações sobre o processo e a linhagem do processo, na descoberta para uma investigação mais aprofundada.

Recomendações de correção:

Se essa atividade for inesperada, seu recurso pode estar comprometido. Para obter mais informações, consulte Como corrigir as descobertas do Monitoramento de runtime.

UnauthorizedAccess:Runtime/TorClient

Sua instância do Amazon EC2 ou um contêiner está fazendo conexões com um Tor Guard ou um nó de autoridade.

Gravidade padrão: alta

- Atributo: Monitoramento de runtime

Essa descoberta informa que um processo em execução na instância EC2 listada ou em um contêiner em seu AWS ambiente está fazendo conexões com um Tor Guard ou um nó de Autoridade. Tor é um software para permitir a comunicação anônima. Tor Guards ou nós de autoridade atuam como gateways iniciais em uma rede do Tor. Esse tráfego pode indicar que a instância do EC2 ou o contêiner foi possivelmente comprometido e está agindo com um cliente em uma rede Tor. Essa descoberta pode indicar acesso não autorizado aos seus AWS recursos com a intenção de ocultar a verdadeira identidade do atacante.

O agente GuardDuty de tempo de execução monitora eventos de vários tipos de recursos. Para identificar o recurso potencialmente comprometido, visualize o tipo de recurso no painel de descobertas no GuardDuty console. Está disponível contexto adicional, incluindo informações sobre o processo e a linhagem do processo, na descoberta para uma investigação mais aprofundada.

Recomendações de correção:

Se essa atividade for inesperada, seu recurso pode estar comprometido. Para obter mais informações, consulte Como corrigir as descobertas do Monitoramento de runtime.

Trojan:Runtime/BlackholeTraffic

Uma instância do Amazon EC2 ou um contêiner está tentando se comunicar com um endereço IP de um host remoto que é um buraco negro conhecido.

Gravidade padrão: média

- Atributo: Monitoramento de runtime

Essa descoberta informa que um processo em execução na instância do EC2 listada ou em um contêiner em seu AWS ambiente pode estar comprometido porque está tentando se comunicar com o endereço IP de um buraco negro (ou sumidouro). Buracos negros são lugares na rede em que o tráfego de entrada ou saída é descartado silenciosamente sem informar à fonte que os dados não chegaram ao destinatário pretendido. Um endereço IP de buraco negro especifica uma máquina host que não está sendo executada ou um endereço para o qual nenhum host foi atribuído.

O agente GuardDuty de tempo de execução monitora eventos de vários tipos de recursos. Para identificar o recurso potencialmente comprometido, visualize o tipo de recurso no painel de

descobertas no GuardDuty console. Está disponível contexto adicional, incluindo informações sobre o processo e a linhagem do processo, na descoberta para uma investigação mais aprofundada.

Recomendações de correção:

Se essa atividade for inesperada, seu recurso pode estar comprometido. Para obter mais informações, consulte Como corrigir as descobertas do Monitoramento de runtime.

Trojan:Runtime/DropPoint

Uma instância do Amazon EC2 ou um contêiner está tentando se comunicar com um endereço IP de um host remoto que é conhecido por manter credenciais e outros dados roubados capturados por malware.

Gravidade padrão: média

- Atributo: Monitoramento de runtime

Essa descoberta informa que um processo em execução na instância do EC2 listada ou em um contêiner em seu AWS ambiente está tentando se comunicar com um endereço IP de um host remoto que é conhecido por conter credenciais e outros dados roubados capturados por malware.

O agente GuardDuty de tempo de execução monitora eventos de vários tipos de recursos. Para identificar o recurso potencialmente comprometido, visualize o tipo de recurso no painel de descobertas no GuardDuty console. Está disponível contexto adicional, incluindo informações sobre o processo e a linhagem do processo, na descoberta para uma investigação mais aprofundada.

Recomendações de correção:

Se essa atividade for inesperada, seu recurso pode estar comprometido. Para obter mais informações, consulte Como corrigir as descobertas do Monitoramento de runtime.

CryptoCurrency:Runtime/BitcoinTool.B! DNS

Uma instância do Amazon EC2 ou um contêiner está consultando um nome de domínio associado a uma atividade de criptomoeda.

Gravidade padrão: alta

- Atributo: Monitoramento de runtime

Essa descoberta informa que um processo em execução na instância do EC2 listada ou um contêiner em seu ambiente da AWS está consultando um nome de domínio associado ao Bitcoin ou a outras atividades relacionadas a criptomoedas. Os agentes de ameaças podem tentar assumir o controle dos recursos computacionais a fim de redirecioná-los de maneira mal-intencionada para a mineração não autorizada de criptomoedas.

O agente GuardDuty de tempo de execução monitora eventos de vários tipos de recursos. Para identificar o recurso potencialmente comprometido, visualize o tipo de recurso no painel de descobertas no GuardDuty console. Está disponível contexto adicional, incluindo informações sobre o processo e a linhagem do processo, na descoberta para uma investigação mais aprofundada.

Recomendações de correção:

Se você usar essa instância do EC2 ou contêiner para minerar ou gerenciar criptomoeda, ou se essa instância ou contêiner estiverem envolvidos de outra forma na atividade de blockchain, a descoberta CryptoCurrency:Runtime/BitcoinTool.B!DNS poderia ser uma atividade esperada para o ambiente. Se esse for o caso em seu AWS ambiente, recomendamos que você configure uma regra de supressão para essa descoberta. A regra de supressão deve consistir em dois critérios de filtro. O primeiro critério deve usar o atributo Tipo de descoberta com um valor de `CryptoCurrency:Runtime/BitcoinTool.B!DNS`. O segundo critério de filtro deve ser o ID de instância da instância ou o ID da imagem do contêiner do contêiner envolvido na atividade de criptomoedas ou blockchain. Para obter mais informações, consulte Regras de supressão.

Se essa atividade for inesperada, seu recurso pode estar comprometido. Para obter mais informações, consulte Como corrigir as descobertas do Monitoramento de runtime.

Backdoor:Runtime/C&CActivity.B! DNS

A instância do Amazon EC2 ou um contêiner está consultando um nome de domínio associado a um servidor de comando e controle conhecido.

Gravidade padrão: alta

- Atributo: Monitoramento de runtime

Essa descoberta informa que um processo em execução na instância do EC2 listada ou o contêiner em seu ambiente da AWS está consultando um nome de domínio associado a um servidor de comando e controle (C&C) conhecido. A instância EC2 listada ou o contêiner podem estar comprometidos. Os servidores de comando e controle são computadores que enviam comandos para membros de um botnet.

Um botnet é uma coleção de dispositivos conectados à Internet, que podem incluir PCs, servidores, dispositivos móveis e dispositivos de Internet das Coisas, infectados e controlados por um tipo comum de malware. Os botnets são frequentemente usados para distribuir malwares e coletar informações inapropriadas, como números de cartão de crédito. Dependendo da finalidade e da estrutura do botnet, o servidor de C&C também pode emitir comandos para iniciar um ataque de negação de serviço distribuída (DDoS).

> **Note**
>
> Se o nome de domínio consultado estiver relacionado ao log4j, os campos da descoberta associada incluirão os seguintes valores:
>
> - `service.additionalInfo.threatListName = Amazon`
> - `service.additionalInfo.threatName = Log4j Related`

> **Note**
>
> Para testar como GuardDuty gera esse tipo de descoberta, você pode fazer uma solicitação de DNS da sua instância (usando `dig` para Linux ou `nslookup` Windows) em um domínio `guarddutyc2activityb.com` de teste.

O agente GuardDuty de tempo de execução monitora eventos de vários tipos de recursos. Para identificar o recurso potencialmente comprometido, visualize o tipo de recurso no painel de descobertas no GuardDuty console. Está disponível contexto adicional, incluindo informações sobre o processo e a linhagem do processo, na descoberta para uma investigação mais aprofundada.

Recomendações de correção:

Se essa atividade for inesperada, seu recurso pode estar comprometido. Para obter mais informações, consulte Como corrigir as descobertas do Monitoramento de runtime.

Trojan:Runtime/BlackholeTraffic! DNS

Uma instância do Amazon EC2 ou um contêiner está consultando um nome de domínio que está sendo redirecionado para o endereço IP de um buraco negro.

Gravidade padrão: média

- Atributo: Monitoramento de runtime

Essa descoberta informa que um processo em execução na instância do EC2 listada ou o contêiner em seu ambiente da AWS pode estar comprometido porque está consultando um nome de domínio que está sendo redirecionado para um endereço IP de buraco negro. Buracos negros são lugares na rede em que o tráfego de entrada ou saída é descartado silenciosamente sem informar à fonte que os dados não chegaram ao destinatário pretendido.

O agente GuardDuty de tempo de execução monitora eventos de vários tipos de recursos. Para identificar o recurso potencialmente comprometido, visualize o tipo de recurso no painel de descobertas no GuardDuty console. Está disponível contexto adicional, incluindo informações sobre o processo e a linhagem do processo, na descoberta para uma investigação mais aprofundada.

Se essa atividade for inesperada, seu recurso pode estar comprometido. Para obter mais informações, consulte Como corrigir as descobertas do Monitoramento de runtime.

Trojan:Runtime/DropPoint! DNS

Uma instância do Amazon EC2 ou um contêiner está consultando um nome de domínio de um host remoto que é conhecido por manter credenciais e outros dados roubados capturados por malware.

Gravidade padrão: média

- Atributo: Monitoramento de runtime

Essa descoberta informa que um processo em execução na instância do EC2 listada ou em um contêiner em seu AWS ambiente está consultando o nome de domínio de um host remoto que é conhecido por conter credenciais e outros dados roubados capturados por malware.

O agente GuardDuty de tempo de execução monitora eventos de vários tipos de recursos. Para identificar o recurso potencialmente comprometido, visualize o tipo de recurso no painel de descobertas no GuardDuty console. Está disponível contexto adicional, incluindo informações sobre o processo e a linhagem do processo, na descoberta para uma investigação mais aprofundada.

Recomendações de correção:

Se essa atividade for inesperada, seu recurso pode estar comprometido. Para obter mais informações, consulte Como corrigir as descobertas do Monitoramento de runtime.

Trojan:Runtime/DGADomainRequest.C! DNS

Uma instância do Amazon EC2 ou um contêiner está consultando domínios gerados por algoritmos. Esses domínios são comumente usados por malware e podem ser um indicativo de uma instância do EC2 ou um contêiner comprometido.

Gravidade padrão: alta

- Atributo: Monitoramento de runtime

Essa descoberta informa que um processo em execução na instância do EC2 listada ou o contêiner no seu ambiente da AWS está tentando consultar domínios do algoritmo de geração de domínio (DGA). Seu recurso pode ter sido comprometido.

Os DGAs são usados para gerar periodicamente uma grande quantidade de nomes de domínio que podem ser usados como pontos de encontro com seus servidores de comando e controle (C&C). Os servidores de comando e controle são computadores que emitem comandos para membros de um botnet, ou seja, uma coleção de dispositivos conectados à Internet infectados e controlados por um tipo comum de malware. Quando há um grande número de possíveis pontos de encontro, isso dificulta o encerramento efetivo dos botnets, uma vez que os computadores infectados tentam entrar em contato com alguns desses nomes de domínio todos os dias para receber atualizações ou comandos.

> **Note**
>
> Essa descoberta é baseada em domínios DGA conhecidos de feeds de inteligência de GuardDuty ameaças.

O agente GuardDuty de tempo de execução monitora eventos de vários tipos de recursos. Para identificar o recurso potencialmente comprometido, visualize o tipo de recurso no painel de descobertas no GuardDuty console. Está disponível contexto adicional, incluindo informações sobre o processo e a linhagem do processo, na descoberta para uma investigação mais aprofundada.

Recomendações de correção:

Se essa atividade for inesperada, seu recurso pode estar comprometido. Para obter mais informações, consulte Como corrigir as descobertas do Monitoramento de runtime.

Trojan:Runtime/DriveBySourceTraffic! DNS

Uma instância do Amazon EC2 ou um contêiner está consultando o nome de domínio de um host remoto que é uma fonte conhecida de ataques de Drive-By download.

Gravidade padrão: alta

- Atributo: Monitoramento de runtime

Essa descoberta informa que um processo em execução na instância do EC2 listada ou o contêiner em seu ambiente da AWS pode estar comprometido porque está consultando um nome de domínio de um host remoto que é uma fonte conhecida de ataques de download drive-by. Estes são downloads indesejados de software de computador da Internet que podem acionar uma instalação automática de vírus, spyware ou malware.

O agente GuardDuty de tempo de execução monitora eventos de vários tipos de recursos. Para identificar o recurso potencialmente comprometido, visualize o tipo de recurso no painel de descobertas no GuardDuty console. Está disponível contexto adicional, incluindo informações sobre o processo e a linhagem do processo, na descoberta para uma investigação mais aprofundada.

Recomendações de correção:

Se essa atividade for inesperada, seu recurso pode estar comprometido. Para obter mais informações, consulte Como corrigir as descobertas do Monitoramento de runtime.

Trojan:Runtime/PhishingDomainRequest! DNS

Uma instância do Amazon EC2 ou um contêiner está consultando domínios envolvidos em ataques de phishing.

Gravidade padrão: alta

- Atributo: Monitoramento de runtime

Essa descoberta informa que um processo em execução na instância do EC2 listada ou um contêiner no seu ambiente da AWS está tentando consultar um domínio envolvido em ataques de phishing. Domínios de phishing são configuradas por alguém se passando por uma instituição legítima para induzir indivíduos a fornecerem dados confidenciais, como informações de identificação pessoal, dados bancários e de cartão de crédito, e senhas. Sua instância do EC2 ou o contêiner

pode estar tentando recuperar dados confidenciais armazenados em um site de phishing ou pode estar tentando configurar um site de phishing. Sua instância do EC2 ou o contêiner pode estar comprometido.

O agente GuardDuty de tempo de execução monitora eventos de vários tipos de recursos. Para identificar o recurso potencialmente comprometido, visualize o tipo de recurso no painel de descobertas no GuardDuty console. Está disponível contexto adicional, incluindo informações sobre o processo e a linhagem do processo, na descoberta para uma investigação mais aprofundada.

Recomendações de correção:

Se essa atividade for inesperada, seu recurso pode estar comprometido. Para obter mais informações, consulte Como corrigir as descobertas do Monitoramento de runtime.

Impact:Runtime/AbusedDomainRequest.Reputation

Uma instância do Amazon EC2 ou um contêiner está consultando um nome de domínio de baixa reputação que está associado a domínios conhecidos por abuso.

Gravidade padrão: média

- Atributo: Monitoramento de runtime

Essa descoberta informa que um processo em execução na instância do EC2 listada ou o contêiner em seu ambiente da AWS está consultando um nome de domínio de baixa reputação associado a domínios ou endereços IP de abuso conhecidos. Exemplos de domínios abusados são nomes de domínio de nível superior (TLDs) e nomes de domínio de segundo nível (2LDs) que fornecem registros gratuitos de subdomínios, bem como provedores de DNS dinâmicos. Os agentes de ameaças tendem a usar esses serviços para registrar domínios gratuitamente ou a baixo custo. Os domínios de baixa reputação nessa categoria também podem ser domínios expirados que se resolvem para o endereço IP estacionário de um registrador e, portanto, podem não estar mais ativas. Um IP de estacionamento é onde um registrador direciona o tráfego para domínios que não foram vinculados a nenhum serviço. A instância listada do Amazon EC2 ou o contêiner podem estar comprometidos, pois os agentes de ameaças geralmente usam esses registradores ou serviços para C&C e distribuição de malware.

Os domínios de baixa reputação são baseados em um modelo de pontuação de reputação. Esse modelo avalia e classifica as características de um domínio para determinar sua probabilidade de ser mal-intencionado.

O agente GuardDuty de tempo de execução monitora eventos de vários tipos de recursos. Para identificar o recurso potencialmente comprometido, visualize o tipo de recurso no painel de descobertas no GuardDuty console. Está disponível contexto adicional, incluindo informações sobre o processo e a linhagem do processo, na descoberta para uma investigação mais aprofundada.

Recomendações de correção:

Se essa atividade for inesperada, seu recurso pode estar comprometido. Para obter mais informações, consulte Como corrigir as descobertas do Monitoramento de runtime.

Impact:Runtime/BitcoinDomainRequest.Reputation

Uma instância do Amazon EC2 ou um contêiner está consultando um nome de domínio associado à atividade relacionada à criptomoeda.

Gravidade padrão: alta

- Atributo: Monitoramento de runtime

Essa descoberta informa que um processo em execução na instância do EC2 listada ou o contêiner em seu ambiente da AWS está consultando um nome de domínio de baixa reputação associado ao Bitcoin ou a outras atividades relacionadas a criptomoedas. Os agentes de ameaças podem tentar assumir o controle dos recursos computacionais para redirecioná-los de maneira mal-intencionada para a mineração não autorizada de criptomoedas.

Os domínios de baixa reputação são baseados em um modelo de pontuação de reputação. Esse modelo avalia e classifica as características de um domínio para determinar sua probabilidade de ser mal-intencionado.

O agente GuardDuty de tempo de execução monitora eventos de vários tipos de recursos. Para identificar o recurso potencialmente comprometido, visualize o tipo de recurso no painel de descobertas no GuardDuty console. Está disponível contexto adicional, incluindo informações sobre o processo e a linhagem do processo, na descoberta para uma investigação mais aprofundada.

Recomendações de correção:

Se você usar essa instância do EC2 ou contêiner para minerar ou gerenciar criptomoeda ou se essa instância estiver envolvida de outra forma na atividade de blockchain, essa descoberta poderia representar a atividade esperada para o ambiente. Se esse for o caso em seu AWS ambiente, recomendamos que você configure uma regra de supressão para essa descoberta. A regra de

supressão deve consistir em dois critérios de filtro. O primeiro critério deve usar o atributo Tipo de descoberta com um valor de `Impact:Runtime/BitcoinDomainRequest.Reputation`. O segundo critério de filtro deve ser o ID da instância ou o ID da imagem do contêiner envolvido em atividades relacionadas à criptomoeda ou blockchain. Para obter mais informações, consulte Regras de supressão.

Se essa atividade for inesperada, seu recurso pode estar comprometido. Para obter mais informações, consulte Como corrigir as descobertas do Monitoramento de runtime.

Impact:Runtime/MaliciousDomainRequest.Reputation

Uma instância do Amazon EC2 ou um contêiner está consultando um domínio de baixa reputação associado a domínios mal-intencionados conhecidos.

Gravidade padrão: alta

- Atributo: Monitoramento de runtime

Essa descoberta informa que um processo em execução na instância do EC2 listada ou o contêiner em seu ambiente da AWS está consultando um nome de domínio de baixa reputação associado a domínios ou endereços IP maliciosos conhecidos. Por exemplo, os domínios podem estar associados a um endereço IP sumidouro conhecido. Domínios sinkholed são domínios que antes eram controlados por um agente de ameaças, e as solicitações feitas a eles podem indicar que a instância está comprometida. Esses domínios também podem estar correlacionados com campanhas mal-intencionadas conhecidas ou algoritmos de geração de domínio.

Os domínios de baixa reputação são baseados em um modelo de pontuação de reputação. Esse modelo avalia e classifica as características de um domínio para determinar sua probabilidade de ser mal-intencionado.

O agente GuardDuty de tempo de execução monitora eventos de vários tipos de recursos. Para identificar o recurso potencialmente comprometido, visualize o tipo de recurso no painel de descobertas no GuardDuty console. Está disponível contexto adicional, incluindo informações sobre o processo e a linhagem do processo, na descoberta para uma investigação mais aprofundada.

Recomendações de correção:

Se essa atividade for inesperada, seu recurso pode estar comprometido. Para obter mais informações, consulte Como corrigir as descobertas do Monitoramento de runtime.

Impact:Runtime/SuspiciousDomainRequest.Reputation

Uma instância do Amazon EC2 ou um contêiner está consultando um nome de domínio de baixa reputação que é suspeito por natureza devido à sua idade ou baixa popularidade.

Gravidade padrão: baixa

- Atributo: Monitoramento de runtime

Essa descoberta informa que um processo em execução na instância do EC2 listada ou o contêiner em seu ambiente da AWS está consultando um nome de domínio de baixa reputação que é suspeito de ser malicioso. As características observadas desse domínio foram consistentes com os domínios maliciosos observados anteriormente. No entanto, nosso modelo de reputação não conseguiu relacioná-lo definitivamente a uma ameaça conhecida. Esses domínios geralmente são observados recentemente ou recebem uma quantidade baixa de tráfego.

Os domínios de baixa reputação são baseados em um modelo de pontuação de reputação. Esse modelo avalia e classifica as características de um domínio para determinar sua probabilidade de ser mal-intencionado.

O agente GuardDuty de tempo de execução monitora eventos de vários tipos de recursos. Para identificar o recurso potencialmente comprometido, visualize o tipo de recurso no painel de descobertas no GuardDuty console. Está disponível contexto adicional, incluindo informações sobre o processo e a linhagem do processo, na descoberta para uma investigação mais aprofundada.

Recomendações de correção:

Se essa atividade for inesperada, seu recurso pode estar comprometido. Para obter mais informações, consulte Como corrigir as descobertas do Monitoramento de runtime.

UnauthorizedAccess:Runtime/MetadataDNSRebind

Uma instância do Amazon EC2 ou um contêiner está executando pesquisas de DNS que são resolvidas como o serviço de metadados da instância.

Gravidade padrão: alta

- Atributo: Monitoramento de runtime

> **Note**
>
> Atualmente, esse tipo de descoberta só é suportado pela arquitetura AMD64.

Essa descoberta informa que um processo em execução na instância do EC2 listada ou em um contêiner em seu AWS ambiente está consultando um domínio que é resolvido para o endereço IP de metadados do EC2 (169.254.169.254). Uma consulta ao DNS desse tipo pode indicar que a instância é alvo de uma técnica de revinculação de DNS. Essa técnica pode ser usada para obter metadados de uma instância do EC2, incluindo as credenciais do IAM associadas à instância.

A revinculação de DNS envolve enganar um aplicativo em execução na instância do EC2 para carregar dados de retorno de um URL, onde o nome de domínio no URL é resolvido como o endereço IP de metadados do EC2 (`169.254.169.254`). Isso faz com que a aplicação acesse metadados do EC2 e possivelmente os disponibilize para o invasor.

É possível acessar metadados do EC2 usando a revinculação de DNS somente se a instância do EC2 estiver executando um aplicativo vulnerável que permita a injeção de URLs ou se um usuário humano acessar a URL em um navegador da web em execução na instância do EC2.

O agente GuardDuty de tempo de execução monitora eventos de vários tipos de recursos. Para identificar o recurso potencialmente comprometido, visualize o tipo de recurso no painel de descobertas no GuardDuty console. Está disponível contexto adicional, incluindo informações sobre o processo e a linhagem do processo, na descoberta para uma investigação mais aprofundada.

Recomendações de correção:

Em resposta a essa descoberta, você deve avaliar se há um aplicativo vulnerável em execução na instância do EC2 ou no contêiner, ou se um usuário humano usou um navegador para acessar o domínio identificado na descoberta. Se a causa raiz for um aplicativo vulnerável, você deverá corrigir a vulnerabilidade. Se for devido à navegação de um usuário no domínio identificado, bloqueie o domínio ou impeça que os usuários o acessem. Se você determinar que essa descoberta estava relacionada a qualquer um dos casos acima, deverá revogar a sessão associada à instância do EC2.

Alguns AWS clientes mapeiam intencionalmente o endereço IP dos metadados para um nome de domínio em seus servidores DNS autorizados. Se esse for o caso em seu ambiente da , recomendamos configurar uma regra de supressão para essa descoberta. A regra de supressão deve consistir em dois critérios de filtro. O primeiro critério deve usar o atributo Tipo de descoberta com um valor de `UnauthorizedAccess:Runtime/MetadataDNSRebind`. O segundo critério

de filtro deve ser o domínio de solicitação de DNS ou o ID da imagem do contêiner. O valor do Domínio da solicitação DNS deve corresponder ao domínio que você mapeou para o endereço IP de metadados (`169.254.169.254`). Para obter informações sobre a criação de regras de supressão, consulte Regras de supressão.

Se essa atividade for inesperada, seu recurso pode estar comprometido. Para obter mais informações, consulte Como corrigir as descobertas do Monitoramento de runtime.

Execution:Runtime/NewBinaryExecuted

Um arquivo binário recém-criado ou modificado recentemente em um contêiner foi executado.

Gravidade padrão: média

- Atributo: Monitoramento de runtime

Essa descoberta informa que um arquivo binário recém-criado ou modificado recentemente em um contêiner foi executado. É a melhor prática manter os contêineres imutáveis em runtime, e arquivos binários, scripts ou bibliotecas não devem ser criados ou modificados durante a vida útil do contêiner. Esse comportamento indica que um agente mal-intencionado potencialmente obteve acesso ao contêiner, baixou e executou malware ou outro software como parte do possível comprometimento. Embora esse tipo de atividade possa ser uma indicação de comprometimento, também é um padrão de uso comum. Portanto, GuardDuty usa mecanismos para identificar instâncias suspeitas dessa atividade e gera esse tipo de descoberta somente para instâncias suspeitas.

O agente GuardDuty de tempo de execução monitora eventos de vários tipos de recursos. Para identificar o recurso potencialmente comprometido, visualize o tipo de recurso no painel de descobertas no GuardDuty console. Para identificar o processo de modificação e o novo binário, veja os detalhes do processo de modificação e os detalhes do processo

Os detalhes do processo de modificação estão incluídos no campo `service.runtimeDetails.context.modifyingProcess` do JSON da descoberta ou em Processo de modificação no painel de detalhes da descoberta. Para esse tipo de descoberta, o processo de modificação é `/usr/bin/dpkg`, conforme identificado pelo campo `service.runtimeDetails.context.modifyingProcess.executablePath` do JSON de descoberta, ou como parte do Processo de modificação no painel de detalhes da descoberta.

Os detalhes do binário novo ou modificado executado estão incluídos no `service.runtimeDetails.process` da descoberta JSON, ou na seção Processo em Detalhes

do runtime. Para esse tipo de descoberta, o binário novo ou modificado é `/usr/bin/python3.8`, conforme indicado pelo campo `service.runtimeDetails.process.executablePath` (Caminho executável).

Recomendações de correção:

Se essa atividade for inesperada, seu recurso pode estar comprometido. Para obter mais informações, consulte Como corrigir as descobertas do Monitoramento de runtime.

PrivilegeEscalation:Runtime/DockerSocketAccessed

Um processo dentro de um contêiner está se comunicando com o daemon do Docker usando o soquete Docker.

Gravidade padrão: média

- Atributo: Monitoramento de runtime

O soquete Docker é um soquete de domínio Unix que o daemon do Docker (`dockerd`) usa para se comunicar com seus clientes. Um cliente pode realizar várias ações, como criar contêineres comunicando-se com o daemon do Docker por meio do soquete do Docker. É suspeito que um processo de contêiner acesse o soquete do Docker. Um processo de contêiner pode escapar do contêiner e obter acesso no nível do host comunicando-se com o soquete do Docker e criando um contêiner privilegiado.

O agente GuardDuty de tempo de execução monitora eventos de vários tipos de recursos. Para identificar o recurso potencialmente comprometido, visualize o tipo de recurso no painel de descobertas no GuardDuty console. Está disponível contexto adicional, incluindo informações sobre o processo e a linhagem do processo, na descoberta para uma investigação mais aprofundada.

Recomendações de correção:

Se essa atividade for inesperada, seu recurso pode estar comprometido. Para obter mais informações, consulte Como corrigir as descobertas do Monitoramento de runtime.

PrivilegeEscalation:Runtime/RuncContainerEscape

Foi detectada uma tentativa de fuga do contêiner por meio do runC.

Gravidade padrão: alta

- Atributo: Monitoramento de runtime

O runC é o runtime de contêiner de baixo nível que os runtimes de contêineres de alto nível, como Docker e Containerd, usam para gerar e executar contêineres. O runC é sempre executado com privilégios de root porque precisa executar a tarefa de baixo nível de criar um contêiner. Um agente de ameaça pode obter acesso no nível do host modificando ou explorando uma vulnerabilidade no binário runC.

Essa descoberta detecta a modificação do binário runC e possíveis tentativas de explorar as seguintes vulnerabilidades do runC:

- CVE-2019-5736— A exploração de CVE-2019-5736 envolve sobrescrever o binário runC de dentro de um contêiner. Essa descoberta é invocada quando o binário runC é modificado por um processo dentro de um contêiner.
- CVE-2024-21626— A exploração de CVE-2024-21626 envolve a configuração do diretório de trabalho atual (CWD) ou de um contêiner como um descritor `/proc/self/fd/`*`FileDescriptor`* de arquivo aberto. Essa descoberta é invocada quando um processo de contêiner com um diretório de trabalho atual abaixo `/proc/self/fd/` é detectado, por exemplo, `/proc/self/fd/7`.

Essa descoberta pode indicar que um agente mal-intencionado tentou realizar a exploração em um dos seguintes tipos de contêineres:

- Um novo contêiner com uma imagem controlada pelo atacante.
- Um contêiner existente que era acessível ao autor com permissões de gravação no binário runC no nível do host.

O agente GuardDuty de tempo de execução monitora eventos de vários tipos de recursos. Para identificar o recurso potencialmente comprometido, visualize o tipo de recurso no painel de descobertas no GuardDuty console.

Recomendações de correção:

Se essa atividade for inesperada, seu recurso pode estar comprometido. Para obter mais informações, consulte Como corrigir as descobertas do Monitoramento de runtime.

PrivilegeEscalation:Runtime/CGroupsReleaseAgentModified

Foi detectada uma tentativa de fuga do contêiner por meio do agente de liberação do CGroups.

Gravidade padrão: alta

- Atributo: Monitoramento de runtime

Essa descoberta informa que foi detectada uma tentativa de modificar um arquivo do agente de liberação do grupo de controle (cgroup). O Linux usa grupos de controle (cgroups) para limitar, contabilizar e isolar o uso de recursos de uma coleção de processos. Cada cgroup tem um arquivo de agente de lançamento (`release_agent`), um script que o Linux executa quando qualquer processo dentro do cgroup é encerrado. O arquivo do agente de liberação é sempre executado no nível do host. Um agente de ameaça dentro de um contêiner pode escapar para o host escrevendo comandos arbitrários no arquivo do agente de lançamento que pertence a um cgroup. Quando um processo dentro desse cgroup termina, os comandos escritos pelo ator são executados.

O agente GuardDuty de tempo de execução monitora eventos de vários tipos de recursos. Para identificar o recurso potencialmente comprometido, visualize o tipo de recurso no painel de descobertas no GuardDuty console.

Recomendações de correção:

Se essa atividade for inesperada, seu recurso pode estar comprometido. Para obter mais informações, consulte Como corrigir as descobertas do Monitoramento de runtime.

DefenseEvasion:Runtime/ProcessInjection.Proc

Uma injeção de processo usando o sistema de arquivos proc foi detectada em um contêiner ou em uma instância do Amazon EC2.

Gravidade padrão: alta

- Atributo: Monitoramento de runtime

A injeção de processos é uma técnica que os agentes de ameaças usam para injetar código nos processos para evitar as defesas e potencialmente elevar os privilégios. O sistema de arquivos proc (procfs) é um sistema de arquivos especial no Linux que apresenta a memória virtual do processo como um arquivo. O caminho desse arquivo é `/proc/PID/mem`, onde `PID` é o ID exclusivo do processo. Um agente de ameaça pode gravar nesse arquivo para injetar código no processo. Essa descoberta identifica possíveis tentativas de gravação nesse arquivo.

O agente GuardDuty de tempo de execução monitora eventos de vários tipos de recursos. Para identificar o recurso potencialmente comprometido, visualize o tipo de recurso no painel de

descobertas no GuardDuty console. Está disponível contexto adicional, incluindo informações sobre o processo e a linhagem do processo, na descoberta para uma investigação mais aprofundada.

Recomendações de correção:

Se essa atividade for inesperada, seu tipo de recurso pode ter sido comprometido. Para obter mais informações, consulte Como corrigir as descobertas do Monitoramento de runtime.

DefenseEvasion:Runtime/ProcessInjection.Ptrace

Uma injeção de processo usando a chamada do sistema ptrace foi detectada em um contêiner ou em uma instância do Amazon EC2.

Gravidade padrão: média

- Atributo: Monitoramento de runtime

A injeção de processos é uma técnica que os agentes de ameaças usam para injetar código nos processos para evitar as defesas e potencialmente elevar os privilégios. Um processo pode usar a chamada do sistema ptrace para injetar código em outro processo. Essa descoberta identifica uma possível tentativa de injetar código em um processo usando a chamada de sistema ptrace.

O agente GuardDuty de tempo de execução monitora eventos de vários tipos de recursos. Para identificar o recurso potencialmente comprometido, visualize o tipo de recurso no painel de descobertas no GuardDuty console. Está disponível contexto adicional, incluindo informações sobre o processo e a linhagem do processo, na descoberta para uma investigação mais aprofundada.

Recomendações de correção:

Se essa atividade for inesperada, seu tipo de recurso pode ter sido comprometido. Para obter mais informações, consulte Como corrigir as descobertas do Monitoramento de runtime.

DefenseEvasion:Runtime/ProcessInjection.VirtualMemoryWrite

Uma injeção de processo por meio de uma gravação direta na memória virtual foi detectada em um contêiner ou em uma instância do Amazon EC2.

Gravidade padrão: alta

- Atributo: Monitoramento de runtime

A injeção de processos é uma técnica que os agentes de ameaças usam para injetar código nos processos para evitar as defesas e potencialmente elevar os privilégios. Um processo pode usar uma chamada de sistema, por exemplo, `process_vm_writev` para injetar código diretamente na memória virtual de outro processo. Essa descoberta identifica uma possível tentativa de injetar código em um processo usando uma chamada de sistema para gravação na memória virtual do processo.

O agente GuardDuty de tempo de execução monitora eventos de vários tipos de recursos. Para identificar o recurso potencialmente comprometido, visualize o tipo de recurso no painel de descobertas no GuardDuty console. Está disponível contexto adicional, incluindo informações sobre o processo e a linhagem do processo, na descoberta para uma investigação mais aprofundada.

Recomendações de correção:

Se essa atividade for inesperada, seu tipo de recurso pode ter sido comprometido. Para obter mais informações, consulte Como corrigir as descobertas do Monitoramento de runtime.

Execution:Runtime/ReverseShell

Um processo em um contêiner ou instância do Amazon EC2 criou um shell reverso.

Gravidade padrão: alta

- Atributo: Monitoramento de runtime

Um shell reverso é uma sessão de shell criada em uma conexão que é iniciada do host de destino para o host do ator. Isso é o oposto de um shell normal iniciado do hospedeiro do agente para o hospedeiro do destino. Os agentes da ameaça criam um shell reverso para executar comandos no alvo depois de obter acesso inicial ao alvo. Essa descoberta identifica conexões de shell reverso potencialmente suspeitas.

GuardDuty examina a atividade e o contexto de tempo de execução relacionados e gera esse tipo de descoberta somente quando a atividade e o contexto associados são considerados incomuns ou suspeitos. Está disponível contexto adicional, incluindo informações sobre o processo e a linhagem do processo, na descoberta para uma investigação mais aprofundada.

Recomendações de correção:

O agente GuardDuty de segurança monitora eventos de várias fontes. Para identificar o recurso afetado, visualize o tipo de recurso nos detalhes da descoberta no GuardDuty console. Se

essa atividade for inesperada, seu tipo de recurso pode ter sido comprometido. Para obter mais informações, consulte Como corrigir as descobertas do Monitoramento de runtime.

DefenseEvasion:Runtime/FilelessExecution

Um processo em um contêiner ou instância do Amazon EC2 está executando código a partir da memória.

Gravidade padrão: média

- Atributo: Monitoramento de runtime

Essa descoberta informa quando um processo é executado usando um arquivo executável na memória no disco. Essa é uma técnica comum de evasão de defesa que evita gravar o executável mal-intencionado no disco para evitar a detecção baseada na verificação do sistema de arquivos. Embora essa técnica seja usada por malware, ela também tem alguns casos de uso legítimos. Um dos exemplos é um compilador just-in-time (JIT) que grava código compilado na memória e o executa a partir da memória.

O agente GuardDuty de tempo de execução monitora eventos de vários tipos de recursos. Para identificar o recurso potencialmente comprometido, visualize o tipo de recurso no painel de descobertas no GuardDuty console. Está disponível contexto adicional, incluindo informações sobre o processo e a linhagem do processo, na descoberta para uma investigação mais aprofundada.

Recomendações de correção:

Se essa atividade for inesperada, seu recurso pode estar comprometido. Para obter mais informações, consulte Como corrigir as descobertas do Monitoramento de runtime.

Impact:Runtime/CryptoMinerExecuted

Um contêiner ou uma instância do Amazon EC2 está executando um arquivo binário associado a uma atividade de mineração de criptomoedas.

Gravidade padrão: alta

- Atributo: Monitoramento de runtime

Essa descoberta informa que um processo em execução na instância ou contêiner do EC2 listado em seu AWS ambiente está executando um arquivo binário associado a uma atividade de

mineração de criptomoedas. Os agentes de ameaças podem tentar assumir o controle dos recursos computacionais para redirecioná-los de maneira mal-intencionada para a mineração não autorizada de criptomoedas.

O agente GuardDuty de tempo de execução monitora eventos de vários tipos de recursos. Para identificar o recurso potencialmente comprometido, visualize o tipo de recurso no painel de descobertas no GuardDuty console. Está disponível contexto adicional, incluindo informações sobre o processo e a linhagem do processo, na descoberta para uma investigação mais aprofundada.

Recomendações de correção:

O agente GuardDuty de tempo de execução monitora eventos de vários recursos. Para identificar o recurso afetado, veja o tipo de recurso nos detalhes das descobertas no GuardDuty console e vejaComo corrigir as descobertas do Monitoramento de runtime.

Execution:Runtime/NewLibraryLoaded

Uma biblioteca recém-criada ou modificada recentemente foi carregada por um processo dentro de um contêiner.

Gravidade padrão: média

- Atributo: Monitoramento de runtime

Essa descoberta informa que uma biblioteca foi criada ou modificada dentro de um contêiner durante o runtime e carregada por um processo executado dentro do contêiner. A melhor prática é manter os contêineres imutáveis no runtime e não criar ou modificar os arquivos binários, scripts ou bibliotecas durante a vida útil do contêiner. O carregamento de uma biblioteca recém-criada ou modificada em um contêiner pode indicar atividade suspeita. Esse comportamento indica que um agente mal-intencionado potencialmente obteve acesso ao contêiner, baixou e executou malware ou outro software como parte do possível comprometimento. Embora esse tipo de atividade possa ser uma indicação de comprometimento, também é um padrão de uso comum. Portanto, GuardDuty usa mecanismos para identificar instâncias suspeitas dessa atividade e gera esse tipo de descoberta somente para instâncias suspeitas.

O agente GuardDuty de tempo de execução monitora eventos de vários recursos. Para identificar o recurso afetado, veja o tipo de recurso nos detalhes das descobertas no GuardDuty console. Está disponível contexto adicional, incluindo informações sobre o processo e a linhagem do processo, na descoberta para uma investigação mais aprofundada.

Recomendações de correção:

Se essa atividade for inesperada, seu recurso pode estar comprometido. Para obter mais informações, consulte Como corrigir as descobertas do Monitoramento de runtime.

PrivilegeEscalation:Runtime/ContainerMountsHostDirectory

Um processo dentro de um contêiner montou um sistema de arquivos hospedeiro em runtime.

Gravidade padrão: média

- Atributo: Monitoramento de runtime

Várias técnicas de escape de contêiner envolvem a montagem de um sistema de arquivos hospedeiro dentro de um contêiner em runtime. Essa descoberta informa que um processo dentro de um contêiner potencialmente tentou montar um sistema de arquivos do host, o que pode indicar uma tentativa de escapar para o host.

O agente GuardDuty de tempo de execução monitora eventos de vários recursos. Para identificar o recurso afetado, veja o tipo de recurso nos detalhes das descobertas no GuardDuty console. Está disponível contexto adicional, incluindo informações sobre o processo e a linhagem do processo, na descoberta para uma investigação mais aprofundada.

Recomendações de correção:

Se essa atividade for inesperada, seu recurso pode estar comprometido. Para obter mais informações, consulte Como corrigir as descobertas do Monitoramento de runtime.

PrivilegeEscalation:Runtime/UserfaultfdUsage

Um processo usou chamadas do sistema **`userfaultfd`** para lidar com falhas de página no espaço do usuário.

Gravidade padrão: média

- Atributo: Monitoramento de runtime

Normalmente, as falhas de página são tratadas pelo kernel no espaço do kernel. No entanto, a chamada de sistema `userfaultfd` permite que um processo manipule falhas de página em um sistema de arquivos no espaço do usuário. Esse é um recurso útil que permite a implementação

de sistemas de arquivos no espaço do usuário. Por outro lado, ele também pode ser usado por um processo potencialmente mal-intencionado para interromper o kernel do espaço do usuário. Interromper o kernel usando a chamada de sistema `userfaultfd` é uma técnica de exploração comum para estender as janelas de corrida durante a exploração das condições de corrida do kernel. O uso de `userfaultfd` pode indicar atividade suspeita na instância do Amazon Elastic Compute Cloud (Amazon EC2).

O agente GuardDuty de tempo de execução monitora eventos de vários recursos. Para identificar o recurso afetado, veja o tipo de recurso nos detalhes das descobertas no GuardDuty console. Está disponível contexto adicional, incluindo informações sobre o processo e a linhagem do processo, na descoberta para uma investigação mais aprofundada.

Recomendações de correção:

Se essa atividade for inesperada, seu recurso pode estar comprometido. Para obter mais informações, consulte Como corrigir as descobertas do Monitoramento de runtime.

Execution:Runtime/SuspiciousTool

Um contêiner ou uma instância do Amazon EC2 está executando um arquivo ou um script binário que é frequentemente usado em cenários de segurança ofensivos, como o engajamento de teste de penetração.

Gravidade padrão: variável

A gravidade dessa descoberta pode ser alta ou baixa, dependendo se a ferramenta suspeita detectada é considerada de uso duplo ou se é exclusivamente para uso ofensivo.

- Atributo: Monitoramento de runtime

Essa descoberta informa que uma ferramenta suspeita foi executada em uma instância ou contêiner do EC2 em seu AWS ambiente. Isso inclui ferramentas usadas em projetos de teste de penetração, também conhecidas como ferramentas de backdoor, scanners de rede e detectores de rede. Todas essas ferramentas podem ser usadas em contextos benignos, mas também são frequentemente usadas por agentes de ameaças com intenções maliciosas. A observação de ferramentas de segurança ofensivas pode indicar que a instância ou o contêiner EC2 associado foi comprometido.

GuardDuty examina a atividade e o contexto de tempo de execução relacionados para gerar essa descoberta somente quando a atividade e o contexto associados forem potencialmente suspeitos.

O agente GuardDuty de tempo de execução monitora eventos de vários recursos. Para identificar o recurso afetado, veja o tipo de recurso nos detalhes das descobertas no GuardDuty console. Quando aplicável, está disponível contexto adicional, bem como informações sobre o processo e a linhagem do processo, para uma investigação mais detalhada.

Recomendações de correção:

Se essa atividade for inesperada, seu recurso pode estar comprometido. Para obter mais informações, consulte Como corrigir as descobertas do Monitoramento de runtime.

Execution:Runtime/SuspiciousCommand

Um comando suspeito foi executado em uma instância do Amazon EC2 ou em um contêiner que indica um comprometimento.

Gravidade padrão: variável

Dependendo do impacto do padrão malicioso observado, a gravidade desse tipo de descoberta pode ser baixa, média ou alta.

- Atributo: Monitoramento de runtime

Essa descoberta informa que um comando suspeito foi executado e indica que uma instância do Amazon EC2 ou um contêiner em AWS seu ambiente foi comprometido. Isso pode significar que um arquivo foi baixado de uma fonte suspeita e depois executado, ou que um processo em execução exibe um padrão malicioso conhecido em sua linha de comando. Isso indica ainda que o malware está sendo executado no sistema.

GuardDuty examina a atividade e o contexto de tempo de execução relacionados para gerar essa descoberta somente quando a atividade e o contexto associados forem potencialmente suspeitos.

O agente GuardDuty de tempo de execução monitora eventos de vários recursos. Para identificar o recurso afetado, veja o tipo de recurso nos detalhes das descobertas no GuardDuty console. Quando aplicável, está disponível contexto adicional, bem como informações sobre o processo e a linhagem do processo, para uma investigação mais detalhada.

Recomendações de correção:

Se essa atividade for inesperada, seu recurso pode estar comprometido. Para obter mais informações, consulte Como corrigir as descobertas do Monitoramento de runtime.

> **Note**
>
> Os argumentos da linha de comando do processo podem conter dados confidenciais. Para proteger dados confidenciais, as descobertas do monitoramento do tempo de GuardDuty execução não incluem argumentos completos da linha de comando. Em vez disso, `Service.RuntimeDetails.Context.CommandLineExample` fornece um exemplo representativo do padrão de linha de comando que gerou a descoberta.

DefenseEvasion:Runtime/SuspiciousCommand

Um comando executado na instância listada do Amazon EC2 ou em um contêiner tenta modificar ou desativar um mecanismo de defesa do Linux, como firewall ou serviços essenciais do sistema.

Gravidade padrão: variável

Dependendo de qual mecanismo de defesa foi modificado ou desativado, a gravidade desse tipo de descoberta pode ser alta, média ou baixa.

- Atributo: Monitoramento de runtime

Essa descoberta informa que um comando que tenta ocultar um ataque dos serviços de segurança do sistema local foi executado. Isso inclui ações como desabilitar o firewall Unix, modificar tabelas IP locais, remover entradas crontab, desabilitar um serviço local ou assumir a função `LDPreload`. Qualquer modificação é altamente suspeita e um potencial indicador de comprometimento. Portanto, esses mecanismos detectam ou evitam maiores comprometimentos do sistema.

GuardDuty examina a atividade e o contexto de tempo de execução relacionados para gerar essa descoberta somente quando a atividade e o contexto associados forem potencialmente suspeitos.

O agente GuardDuty de tempo de execução monitora eventos de vários recursos. Para identificar o recurso potencialmente comprometido, veja o tipo de recurso nos detalhes das descobertas no GuardDuty console. Quando aplicável, está disponível contexto adicional, bem como informações sobre o processo e a linhagem do processo, para uma investigação mais detalhada.

Recomendações de correção:

Se essa atividade for inesperada, seu recurso pode estar comprometido. Para obter mais informações, consulte Como corrigir as descobertas do Monitoramento de runtime.

DefenseEvasion:Runtime/PtraceAntiDebugging

Um processo em um contêiner ou instância do Amazon EC2 executou uma medida de antidepuração usando a chamada do sistema ptrace.

Gravidade padrão: baixa

- Atributo: Monitoramento de runtime

Essa descoberta mostra que um processo em execução na instância do Amazon EC2 listada ou um contêiner em seu ambiente da AWS usou a chamada do sistema ptrace com a opção `PTRACE_TRACEME`. Essa atividade faria com que um depurador conectado se separasse do processo em execução. De outra forma, se não houver um depurador conectado, ela não terá efeito. No entanto, a atividade por si só levanta suspeitas. Isso indica ainda que o malware está sendo executado no sistema. O malware frequentemente usa técnicas de antidepuração para evitar a análise, e essas técnicas podem ser detectadas em runtime.

GuardDuty examina a atividade e o contexto de tempo de execução relacionados para gerar essa descoberta somente quando a atividade e o contexto associados forem potencialmente suspeitos.

O agente GuardDuty de tempo de execução monitora eventos de vários recursos. Para identificar o recurso afetado, veja o tipo de recurso nos detalhes das descobertas no GuardDuty console. Está disponível contexto adicional, incluindo informações sobre o processo e a linhagem do processo, na descoberta para uma investigação mais aprofundada.

Recomendações de correção:

Se essa atividade for inesperada, seu recurso pode estar comprometido. Para obter mais informações, consulte Como corrigir as descobertas do Monitoramento de runtime.

Execution:Runtime/MaliciousFileExecuted

Um arquivo executável malicioso conhecido foi executado em uma instância do Amazon EC2 ou em um contêiner.

Gravidade padrão: alta

- Atributo: Monitoramento de runtime

Essa descoberta informa que um executável malicioso conhecido foi executado na instância do Amazon EC2 ou em um contêiner dentro do seu ambiente. AWS Esse é um forte indicador de que a instância ou o contêiner foram potencialmente comprometidos e que o malware foi executado.

GuardDuty examina a atividade e o contexto de tempo de execução relacionados para gerar essa descoberta somente quando a atividade e o contexto associados forem potencialmente suspeitos.

O agente GuardDuty de tempo de execução monitora eventos de vários recursos. Para identificar o recurso afetado, veja o tipo de recurso nos detalhes das descobertas no GuardDuty console. Quando aplicável, está disponível contexto adicional, bem como informações sobre o processo e a linhagem do processo, para uma investigação mais detalhada.

Recomendações de correção:

Se essa atividade for inesperada, seu recurso pode estar comprometido. Para obter mais informações, consulte Como corrigir as descobertas do Monitoramento de runtime.

Execution:Runtime/MaliciousFileExecuted.Custom

Um arquivo executável mal-intencionado em uma lista personalizada de ameaças foi executado em um contêiner ou uma instância do Amazon EC2.

Gravidade padrão: alta

- Atributo: Monitoramento de runtime

Essa descoberta informa que um arquivo executável incluído em uma lista de entidades de ameaça que você carregou e ativou foi executado em uma instância do Amazon EC2 ou em um contêiner em seu ambiente. AWS Em GuardDuty, uma lista de entidades de ameaça pode incluir endereços IP, domínios e hashes de SHA-256 arquivos maliciosos conhecidos. GuardDuty gera descobertas com base na atividade associada à lista de entidades ameaçadoras carregada. É possível visualizar o nome dessa lista de entidades de ameaças nos detalhes da descoberta.

Observação: essa descoberta só é acionada quando um arquivo executável cujo hash foi incluído na lista de entidades de ameaça é executado.

O agente GuardDuty de tempo de execução monitora eventos de vários recursos. Para identificar o recurso afetado, veja o tipo de recurso nos detalhes das descobertas no GuardDuty console. Quando aplicável, está disponível contexto adicional, bem como informações sobre o processo e a linhagem do processo, para uma investigação mais detalhada.

Recomendações de correção:

Se essa atividade for inesperada, seu recurso pode estar comprometido. Para obter mais informações, consulte Como corrigir as descobertas do Monitoramento de runtime.

Execution:Runtime/SuspiciousShellCreated

Um serviço de rede ou processo acessível pela rede em uma instância do Amazon EC2 ou em um contêiner iniciou um processo de shell interativo.

Gravidade padrão: baixa

- Atributo: Monitoramento de runtime

Essa descoberta informa que um serviço acessível pela rede em uma instância do Amazon EC2 ou em um contêiner dentro do seu AWS ambiente lançou um shell interativo. Sob certas circunstâncias, esse cenário pode indicar um comportamento pós-exploração. Os shells interativos permitem que os invasores executem comandos arbitrários em uma instância ou contêiner comprometido.

O agente GuardDuty de tempo de execução monitora eventos de vários recursos. Para identificar o recurso afetado, veja o tipo de recurso nos detalhes das descobertas no GuardDuty console. Está disponível contexto adicional, incluindo informações sobre o processo e a linhagem do processo, na descoberta para uma investigação mais aprofundada. Você pode visualizar as informações do processo acessível pela rede nos detalhes do processo principal.

Recomendações de correção:

Se essa atividade for inesperada, seu recurso pode estar comprometido. Para obter mais informações, consulte Como corrigir as descobertas do Monitoramento de runtime.

PrivilegeEscalation:Runtime/ElevationToRoot

Um processo em execução na instância ou contêiner listado do Amazon EC2 assumiu privilégios de root.

Gravidade padrão: média

- Atributo: Monitoramento de runtime

Essa descoberta informa que um processo em execução no Amazon EC2 listado ou no contêiner listado em AWS seu ambiente assumiu privilégios de root por meio de execução binária incomum

ou `setuid` suspeita. Isso indica que um processo em execução foi potencialmente comprometido, para a instância do EC2 por meio de uma exploração ou por meio de exploração `setuid`. Ao usar os privilégios de root, o invasor pode potencialmente executar comandos na instância ou no contêiner.

Embora tenha sido GuardDuty projetado para não gerar esse tipo de descoberta para atividades que envolvam o uso regular do `sudo` comando, ele gerará essa descoberta quando identificar a atividade como incomum ou suspeita.

GuardDuty examina a atividade e o contexto relacionados ao tempo de execução e gera esse tipo de descoberta somente quando a atividade e o contexto associados são incomuns ou suspeitos.

O agente GuardDuty de tempo de execução monitora eventos de vários recursos. Para identificar o recurso afetado, veja o tipo de recurso nos detalhes das descobertas no GuardDuty console. Está disponível contexto adicional, incluindo informações sobre o processo e a linhagem do processo, na descoberta para uma investigação mais aprofundada.

Recomendações de correção:

Se essa atividade for inesperada, seu recurso pode estar comprometido. Para obter mais informações, consulte Como corrigir as descobertas do Monitoramento de runtime.

Discovery:Runtime/SuspiciousCommand

Um comando suspeito foi executado em uma instância do Amazon EC2 ou em um contêiner, o que permite que um invasor obtenha informações sobre o sistema local, ao redor AWS infraestrutura ou infraestrutura de contêineres.

Gravidade padrão: baixa

Atributo: Monitoramento de runtime

Essa descoberta informa que um processo em execução na instância listada do Amazon EC2 ou um contêiner em seu ambiente da AWS executou um comando que pode fornecer a um invasor informações cruciais para potencialmente avançar no ataque. As seguintes informações podem ter sido recuperadas:

- Sistema local, como configuração de usuário ou rede,
- Outros AWS recursos e permissões disponíveis, ou
- Infraestrutura do Kubernetes, como serviços e pods.

A instância do Amazon EC2 ou o contêiner que está listado nos detalhes da descoberta pode ter sido comprometido.

O agente GuardDuty de tempo de execução monitora eventos de vários tipos de recursos. Para identificar o recurso potencialmente comprometido, veja o tipo de recurso nos detalhes das descobertas no GuardDuty console. Você pode encontrar os detalhes sobre o comando suspeito no campo `service.runtimeDetails.context` da descoberta JSON. Está disponível contexto adicional, incluindo informações sobre o processo e a linhagem do processo, na descoberta para uma investigação mais aprofundada.

Recomendações de correção:

Se essa atividade for inesperada, seu recurso pode estar comprometido. Para obter mais informações, consulte Como corrigir as descobertas do Monitoramento de runtime.

Persistence:Runtime/SuspiciousCommand

Um comando suspeito foi executado em uma instância do Amazon EC2 ou em um contêiner, o que permite que um invasor persista o acesso e o controle em seu AWS meio ambiente.

Gravidade padrão: média

- Atributo: Monitoramento de runtime

Essa descoberta informa que um processo em execução na instância listada do Amazon EC2 ou em um contêiner em AWS seu ambiente executou um comando suspeito. O comando instala um método de persistência que permite que o malware seja executado ininterruptamente ou permite que um invasor acesse continuamente a instância ou o tipo de recurso de contêiner potencialmente comprometido. Isso pode significar que um serviço do sistema foi instalado ou modificado, que `crontab` foi modificado ou que um novo usuário foi adicionado à configuração do sistema.

GuardDuty examina a atividade e o contexto relacionados ao tempo de execução e gera esse tipo de descoberta somente quando a atividade e o contexto associados são incomuns ou suspeitos.

A instância do Amazon EC2 ou o contêiner que está listado nos detalhes da descoberta pode ter sido comprometido.

O agente GuardDuty de tempo de execução monitora eventos de vários recursos. Para identificar o recurso potencialmente comprometido, veja o tipo de recurso nos detalhes das descobertas

no GuardDuty console. Você pode encontrar os detalhes sobre o comando suspeito no campo `service.runtimeDetails.context` da descoberta JSON. Quando aplicável, está disponível contexto adicional, bem como informações sobre o processo e a linhagem do processo, para uma investigação mais detalhada.

Recomendações de correção:

Se essa atividade for inesperada, seu recurso pode estar comprometido. Para obter mais informações, consulte Como corrigir as descobertas do Monitoramento de runtime.

PrivilegeEscalation:Runtime/SuspiciousCommand

Um comando suspeito foi executado em uma instância do Amazon EC2 ou em um contêiner, o que permite que um invasor aumente seus privilégios.

Gravidade padrão: média

- Atributo: Monitoramento de runtime

Essa descoberta informa que um processo em execução na instância listada do Amazon EC2 ou em um contêiner em AWS seu ambiente executou um comando suspeito. O comando tenta realizar o escalonamento de privilégios, o que permite que um adversário execute tarefas de alto privilégio.

GuardDuty examina a atividade e o contexto relacionados ao tempo de execução e gera esse tipo de descoberta somente quando a atividade e o contexto associados são incomuns ou suspeitos.

A instância do Amazon EC2 ou o contêiner que está listado nos detalhes da descoberta pode ter sido comprometido.

O agente GuardDuty de tempo de execução monitora eventos de vários recursos. Para identificar o recurso afetado, veja o tipo de recurso nos detalhes das descobertas no GuardDuty console. Quando aplicável, está disponível contexto adicional, bem como informações sobre o processo e a linhagem do processo, para uma investigação mais detalhada.

Recomendações de correção:

Se essa atividade for inesperada, seu recurso pode estar comprometido. Para obter mais informações, consulte Como corrigir as descobertas do Monitoramento de runtime.

DefenseEvasion:Runtime/KernelModuleLoaded

Um módulo do kernel foi carregado em uma instância do Amazon EC2, indicando uma tentativa de obter acesso no nível do kernel.

Gravidade padrão: alta

- Atributo: Monitoramento de runtime

Essa descoberta indica que um módulo do kernel foi carregado na instância do EC2 listada. Como os módulos do kernel têm os privilégios mais altos em nível de sistema (anel 0), isso pode indicar que um agente de ameaças obteve acesso em nível de kernel. Esse nível de acesso permite controle total sobre o sistema.

O agente GuardDuty de tempo de execução monitora eventos de vários recursos. Para identificar o recurso afetado, veja o tipo de recurso nos detalhes das descobertas no GuardDuty console. Quando aplicável, está disponível contexto adicional, bem como informações sobre o processo e a linhagem do processo, para uma investigação mais detalhada.

Recomendações de correção:

Se essa atividade for inesperada, seu recurso pode estar comprometido. Para obter mais informações, consulte Como corrigir as descobertas do Monitoramento de runtime.

Persistence:Runtime/SensitiveFileModified

Um arquivo de sistema sensível à segurança foi modificado em uma instância ou um contêiner do Amazon EC2, o que pode permitir que um invasor obtenha persistência.

Gravidade padrão: média

- Atributo: Monitoramento de runtime

Essa descoberta informa que um arquivo de sistema sensível à segurança em uma instância ou um contêiner do Amazon EC2 foi modificado, o que pode permitir que um invasor mantenha direitos de execução persistentes no sistema. Isso pode incluir a instalação de novos arquivos de chave SSH, alterações nos arquivos de configuração do usuário, modificações nos arquivos de senha ou sombra, criação de tarefas programadas, manipulação de scripts de inicialização do sistema ou modificação de arquivos executáveis ou de script por processos de serviços da Web em contextos suspeitos.

Essas modificações são indicadores de comprometimento que podem permitir a persistência não autorizada em seu ambiente.

GuardDuty monitora a persistência de arquivos de sistema sensíveis à segurança, frequentemente alvos de adversários. Como esses arquivos também podem ser modificados durante a administração e o gerenciamento legítimos do sistema, GuardDuty examina a atividade e o contexto de tempo de execução relacionados para gerar essa descoberta somente quando as modificações são correlacionadas a outras atividades suspeitas.

O agente GuardDuty de tempo de execução monitora eventos de vários tipos de recursos. Para identificar o recurso potencialmente comprometido, visualize o tipo de recurso no painel de descobertas no GuardDuty console. O campo `service.runtimeDetails.context` contém detalhes sobre a modificação suspeita do arquivo, incluindo o caminho do arquivo e o tipo de operação.

Recomendações de correção:

Se essa atividade for inesperada, seu recurso pode estar comprometido. Para obter mais informações, consulte Como corrigir as descobertas do Monitoramento de runtime.

PrivilegeEscalation:Runtime/SensitiveFileModified

Um arquivo de sistema sensível à segurança foi modificado em uma instância ou um contêiner do Amazon EC2, o que pode permitir que um invasor tenha mais privilégios.

Gravidade padrão: média

- Atributo: Monitoramento de runtime

Essa descoberta informa que um arquivo de sistema sensível à segurança foi modificado em uma instância ou um contêiner do Amazon EC2, o que pode permitir que um invasor tenha mais privilégios no sistema. Isso pode envolver modificações em arquivos essenciais à segurança, como configuração do sudoers, configurações do PAM ou arquivos de autenticação do sistema. Essas modificações são indicadores de comprometimento que podem permitir o aumento não autorizado de privilégios, possivelmente resultando em acesso raiz não autorizado, mecanismos de autenticação enfraquecidos ou controles de segurança comprometidos.

GuardDuty monitora arquivos de sistema sensíveis à segurança, frequentemente alvos de adversários para aumentar os privilégios. Como esses arquivos também podem ser modificados

durante a administração e o gerenciamento legítimos do sistema, GuardDuty examina a atividade e o contexto de tempo de execução relacionados para gerar essa descoberta somente quando as modificações são correlacionadas a outras atividades suspeitas.

O agente GuardDuty de tempo de execução monitora eventos de vários tipos de recursos. Para identificar o recurso potencialmente comprometido, visualize o tipo de recurso no painel de descobertas no GuardDuty console. O campo `service.runtimeDetails.context` contém detalhes sobre a modificação suspeita do arquivo, incluindo o caminho do arquivo e o tipo de operação.

Recomendações de correção:

Se essa atividade for inesperada, seu recurso pode estar comprometido. Para obter mais informações, consulte Como corrigir as descobertas do Monitoramento de runtime.

DefenseEvasion:Runtime/SensitiveFileModified

Um arquivo de sistema sensível à segurança foi modificado em uma instância ou um contêiner do Amazon EC2, o que pode permitir que um invasor escape da detecção.

Gravidade padrão: média

- Atributo: Monitoramento de runtime

Essa descoberta informa que um arquivo de sistema sensível à segurança em uma instância ou um contêiner do Amazon EC2 foi modificado, o que pode permitir que um invasor escape da detecção no sistema. Isso pode envolver modificações nos arquivos de log do sistema, nas configurações de auditoria, nos arquivos do histórico de comandos ou nos logs do sistema. Essas modificações são indicadores de comprometimento que podem permitir a ocultação de atividades não autorizadas, a interrupção do monitoramento de segurança ou a remoção de evidências de atividades do sistema.

GuardDuty monitora arquivos de sistema sensíveis à segurança, frequentemente alvos de adversários para evasão de defesa. Como esses arquivos também podem ser modificados durante a administração e o gerenciamento legítimos do sistema, GuardDuty examina a atividade e o contexto de tempo de execução relacionados para gerar essa descoberta somente quando as modificações são correlacionadas a outras atividades suspeitas.

O agente GuardDuty de tempo de execução monitora eventos de vários tipos de recursos. Para identificar o recurso potencialmente comprometido, visualize o tipo de recurso no painel de

descobertas no GuardDuty console. O campo `service.runtimeDetails.context` contém detalhes sobre a modificação suspeita do arquivo, incluindo o caminho do arquivo e o tipo de operação.

Recomendações de correção:

Se essa atividade for inesperada, seu recurso pode estar comprometido. Para obter mais informações, consulte Como corrigir as descobertas do Monitoramento de runtime.

Encontrando tipos que exigem regras de detecção personalizadas

GuardDuty gera os seguintes tipos de descoberta somente quando você ativa as Regras de Detecção Personalizadas para Monitoramento de Tempo de Execução. Para obter mais informações, consulte Regras de detecção personalizadas em GuardDuty.

Cada descoberta inclui o `CustomDetectionRuleName` campo, que contém o nome da regra que gerou a descoberta.

Tópicos

- CommandAndControl:Runtime/SuspiciousCommand
- CredentialAccess:Runtime/SensitiveFileRead
- Discovery:Runtime/SensitiveFileRead
- Exfiltration:Runtime/SuspiciousCommand

CommandAndControl:Runtime/SuspiciousCommand

Um processo em uma instância do Amazon EC2 ou em um contêiner executou um comando suspeito que um invasor poderia usar para se comunicar e controlar o recurso.

Gravidade padrão: variável

A severidade depende da regra que gerou a descoberta: alta para DnsTunnelingToolExecuted e média paraSuspiciousProtocolTunneling.

- Atributo: Monitoramento de runtime

Essa descoberta informa que um processo em uma instância ou contêiner do Amazon EC2 em AWS seu ambiente executou um comando que um invasor poderia usar para se comunicar com

um recurso comprometido, evitando a detecção. Por exemplo, o processo pode ter executado uma ferramenta que encaminha o tráfego pelo DNS ou que expõe o recurso por meio de um túnel ou serviço de proxy.

GuardDuty gera essa descoberta a partir SuspiciousProtocolTunneling das regras DnsTunnelingToolExecuted e.

Recomendações de correção:

Se essa atividade for inesperada, seu recurso pode estar comprometido. Para obter mais informações, consulte Como corrigir as descobertas do Monitoramento de runtime.

CredentialAccess:Runtime/SensitiveFileRead

Um processo em uma instância do Amazon EC2 ou em um contêiner acessou um arquivo confidencial que pode conter credenciais.

Gravidade padrão: alta

- Atributo: Monitoramento de runtime

Essa descoberta informa que um processo em uma instância ou contêiner do Amazon EC2 em AWS seu ambiente acessou um arquivo sensível à segurança que pode conter credenciais ou outros segredos. Por exemplo, o processo pode ter acessado a memória de outro processo por meio do sistema de `/proc` arquivos para extrair credenciais dele.

GuardDuty gera essa descoberta a partir da DumpProcessMemoryFromProc regra.

Recomendações de correção:

Se essa atividade for inesperada, seu recurso pode estar comprometido. Para obter mais informações, consulte Como corrigir as descobertas do Monitoramento de runtime.

Discovery:Runtime/SensitiveFileRead

Um processo em uma instância do Amazon EC2 ou em um contêiner acessou um arquivo confidencial que contém informações sobre usuários e credenciais locais.

Gravidade padrão: média

- Atributo: Monitoramento de runtime

Essa descoberta informa que um processo em uma instância ou contêiner do Amazon EC2 em AWS seu ambiente acessou um arquivo de sistema sensível à segurança, como a conta de usuário local ou arquivos hash de senha. Um invasor pode usar essas informações para descobrir contas e tentar decifrar suas senhas.

GuardDuty gera essa descoberta a partir da PasswordShadowFileDiscovery regra.

Recomendações de correção:

Se essa atividade for inesperada, seu recurso pode estar comprometido. Para obter mais informações, consulte Como corrigir as descobertas do Monitoramento de runtime.

Exfiltration:Runtime/SuspiciousCommand

Um processo em uma instância do Amazon EC2 ou em um contêiner executou um comando suspeito que um invasor poderia usar para mover dados para fora do seu ambiente.

Gravidade padrão: média

- Atributo: Monitoramento de runtime

Essa descoberta informa que um processo em uma instância ou contêiner do Amazon EC2 em AWS seu ambiente executou um comando que poderia ser usado para mover dados para fora do seu ambiente. Por exemplo, o processo pode ter carregado um arquivo em um terminal externo ou em um serviço de armazenamento em nuvem ou dividido os dados em partes menores para evitar limites de transferência.

GuardDuty gera essa descoberta a partir das S3DataExfiltrationWithRclone regras CurlWgetExfiltrateDataDataSplittingForExfiltration, e.

Recomendações de correção:

Se essa atividade for inesperada, seu recurso pode estar comprometido. Para obter mais informações, consulte Como corrigir as descobertas do Monitoramento de runtime.

Tipos de descoberta da Proteção contra malware para EC2

GuardDuty O Malware Protection for EC2 fornece uma única proteção contra malware para o EC2, detectando todas as ameaças detectadas durante a verificação de uma instância do EC2 ou de uma carga de trabalho de contêiner. A descoberta inclui o número total de detecções feitas durante

a verificação e fornece detalhes das 32 principais ameaças detectadas com base na gravidade. Diferentemente de outras GuardDuty descobertas, as descobertas do Malware Protection for EC2 não são atualizadas quando a mesma instância do EC2 ou carga de trabalho do contêiner é verificada novamente.

Uma nova descoberta da Proteção contra malware para EC2 é gerada para cada verificação que detecta malware. As descobertas do Malware Protection for EC2 incluem informações sobre a verificação correspondente que produziu a descoberta, bem como a GuardDuty descoberta que iniciou essa verificação. Isso facilita correlacionar o comportamento suspeito com o malware detectado.

> **Note**
>
> Quando GuardDuty detecta atividades maliciosas em uma carga de trabalho de contêiner, o Malware Protection for EC2 não gera uma descoberta no nível do EC2.

As descobertas a seguir são específicas da Proteção contra GuardDuty Malware para EC2.

Tópicos

- Execution:EC2/MaliciousFile
- Execution:ECS/MaliciousFile
- Execution:Kubernetes/MaliciousFile
- Execution:Container/MaliciousFile
- Execution:EC2/SuspiciousFile
- Execution:ECS/SuspiciousFile
- Execution:Kubernetes/SuspiciousFile
- Execution:Container/SuspiciousFile

Execution:EC2/MaliciousFile

Um arquivo mal-intencionado foi detectado em uma instância do EC2.

Gravidade padrão: varia de acordo com a ameaça detectada.

- Atributo: Proteção contra malware EBS

Essa descoberta indica que a verificação do GuardDuty Malware Protection for EC2 detectou um ou mais arquivos maliciosos na instância do EC2 listada em seu AWS ambiente. Essa instância listada pode estar comprometida. Para obter mais informações, consulte a seção Ameaças detectadas nos detalhes das descobertas.

Recomendações de correção:

Se essa atividade for inesperada, sua instância pode estar comprometida. Para obter mais informações, consulte Como corrigir uma instância do Amazon EC2 potencialmente comprometida.

Execution:ECS/MaliciousFile

Um arquivo mal-intencionado foi detectado em um cluster do ECS.

Gravidade padrão: varia de acordo com a ameaça detectada.

- Atributo: Proteção contra malware EBS

Essa descoberta indica que a verificação do GuardDuty Malware Protection for EC2 detectou um ou mais arquivos maliciosos em uma carga de trabalho de contêiner que pertence a um cluster ECS. Para obter mais informações, consulte a seção Ameaças detectadas nos detalhes das descobertas.

Recomendações de correção:

Se essa atividade for inesperada, seu contêiner pertencente ao cluster ECS poderá ser comprometido. Para obter mais informações, consulte Como corrigir um cluster do ECS possivelmente comprometido.

Execution:Kubernetes/MaliciousFile

Um arquivo mal-intencionado foi detectado em um cluster do Kubernetes.

Gravidade padrão: varia de acordo com a ameaça detectada.

- Atributo: Proteção contra malware EBS

Essa descoberta indica que a verificação do GuardDuty Malware Protection for EC2 detectou um ou mais arquivos maliciosos em uma carga de trabalho de contêiner que pertence a um cluster Kubernetes. Se for um cluster gerenciado pelo EKS, os detalhes das descobertas fornecerão mais

informações sobre o recurso do EKS afetado. Para obter mais informações, consulte a seção Ameaças detectadas nos detalhes das descobertas.

Recomendações de correção:

Se essa atividade for inesperada, a workload do contêiner poderá ser comprometida. Para obter mais informações, consulte Como corrigir as descobertas da Proteção do EKS.

Execution:Container/MaliciousFile

Um arquivo mal-intencionado foi detectado em um contêiner independente.

Gravidade padrão: varia de acordo com a ameaça detectada.

- Atributo: Proteção contra malware EBS

Essa descoberta indica que a verificação do GuardDuty Malware Protection for EC2 detectou um ou mais arquivos maliciosos na carga de trabalho de um contêiner e nenhuma informação do cluster foi identificada. Para obter mais informações, consulte a seção Ameaças detectadas nos detalhes das descobertas.

Recomendações de correção:

Se essa atividade for inesperada, a workload do contêiner poderá ser comprometida. Para obter mais informações, consulte Como corrigir um contêiner autônomo possivelmente comprometido.

Execution:EC2/SuspiciousFile

Um arquivo suspeito foi detectado em uma instância do EC2.

Gravidade padrão: varia de acordo com a ameaça detectada.

- Atributo: Proteção contra malware EBS

Essa descoberta indica que a verificação do GuardDuty Malware Protection for EC2 detectou um ou mais arquivos suspeitos em uma instância do EC2. Para obter mais informações, consulte a seção Ameaças detectadas nos detalhes das descobertas.

As detecções de tipo `SuspiciousFile` indicam que programas potencialmente indesejados, como adware, spyware ou ferramentas de uso duplo, estão presentes em um recurso afetado. Esses

programas podem ter um impacto negativo em seus recursos ou ser usados por invasores para fins mal-intencionados. Por exemplo, ferramentas de rede podem ser usadas de forma legítima ou maliciosa por adversários como ferramentas de hack para tentar comprometer recursos.

Quando um arquivo suspeito for detectado, avalie se você espera ver o arquivo detectado em seu AWS ambiente. Se o arquivo for inesperado, siga as recomendações de correção fornecidas na próxima seção.

Recomendações de correção:

Se essa atividade for inesperada, sua instância pode estar comprometida. Para obter mais informações, consulte Como corrigir uma instância do Amazon EC2 potencialmente comprometida.

Execution:ECS/SuspiciousFile

Um arquivo suspeito foi detectado em um cluster do ECS.

Gravidade padrão: varia de acordo com a ameaça detectada.

- Atributo: Proteção contra malware EBS

Essa descoberta indica que a verificação do GuardDuty Malware Protection for EC2 detectou um ou mais arquivos suspeitos em um contêiner que pertence a um cluster ECS. Para obter mais informações, consulte a seção Ameaças detectadas nos detalhes das descobertas.

As detecções de tipo `SuspiciousFile` indicam que programas potencialmente indesejados, como adware, spyware ou ferramentas de uso duplo, estão presentes em um recurso afetado. Esses programas podem ter um impacto negativo em seus recursos ou ser usados por invasores para fins mal-intencionados. Por exemplo, ferramentas de rede podem ser usadas de forma legítima ou maliciosa por adversários como ferramentas de hack para tentar comprometer recursos.

Quando um arquivo suspeito for detectado, avalie se você espera ver o arquivo detectado em seu AWS ambiente. Se o arquivo for inesperado, siga as recomendações de correção fornecidas na próxima seção.

Recomendações de correção:

Se essa atividade for inesperada, seu contêiner pertencente ao cluster ECS poderá ser comprometido. Para obter mais informações, consulte Como corrigir um cluster do ECS possivelmente comprometido.

Execution:Kubernetes/SuspiciousFile

Um arquivo suspeito foi detectado em um cluster do Kubernetes.

Gravidade padrão: varia de acordo com a ameaça detectada.

- Atributo: Proteção contra malware EBS

Essa descoberta indica que a verificação do GuardDuty Malware Protection for EC2 detectou um ou mais arquivos suspeitos em um contêiner que pertence a um cluster Kubernetes. Se for um cluster gerenciado pelo EKS, os detalhes das descobertas fornecerão mais informações sobre o EKS afetado. Para obter mais informações, consulte a seção Ameaças detectadas nos detalhes das descobertas.

As detecções de tipo `SuspiciousFile` indicam que programas potencialmente indesejados, como adware, spyware ou ferramentas de uso duplo, estão presentes em um recurso afetado. Esses programas podem ter um impacto negativo em seus recursos ou ser usados por invasores para fins mal-intencionados. Por exemplo, ferramentas de rede podem ser usadas de forma legítima ou maliciosa por adversários como ferramentas de hack para tentar comprometer recursos.

Quando um arquivo suspeito for detectado, avalie se você espera ver o arquivo detectado em seu AWS ambiente. Se o arquivo for inesperado, siga as recomendações de correção fornecidas na próxima seção.

Recomendações de correção:

Se essa atividade for inesperada, a workload do contêiner poderá ser comprometida. Para obter mais informações, consulte Como corrigir as descobertas da Proteção do EKS.

Execution:Container/SuspiciousFile

Um arquivo suspeito foi detectado em um contêiner independente.

Gravidade padrão: varia de acordo com a ameaça detectada.

- Atributo: Proteção contra malware EBS

Essa descoberta indica que a verificação do GuardDuty Malware Protection for EC2 detectou um ou mais arquivos suspeitos em um contêiner sem informações de cluster. Para obter mais informações, consulte a seção Ameaças detectadas nos detalhes das descobertas.

As detecções de tipo `SuspiciousFile` indicam que programas potencialmente indesejados, como adware, spyware ou ferramentas de uso duplo, estão presentes em um recurso afetado. Esses programas podem ter um impacto negativo em seus recursos ou ser usados por invasores para fins mal-intencionados. Por exemplo, ferramentas de rede podem ser usadas de forma legítima ou maliciosa por adversários como ferramentas de hack para tentar comprometer recursos.

Quando um arquivo suspeito for detectado, avalie se você espera ver o arquivo detectado em seu AWS ambiente. Se o arquivo for inesperado, siga as recomendações de correção fornecidas na próxima seção.

Recomendações de correção:

Se essa atividade for inesperada, a workload do contêiner poderá ser comprometida. Para obter mais informações, consulte Como corrigir um contêiner autônomo possivelmente comprometido.

Tipo de descoberta da Proteção contra malware para S3

GuardDuty gera uma descoberta somente quando detecta uma possível ameaça à segurança em seu Conta da AWS. Uma descoberta da Proteção contra malware para S3 indica que o objeto carregado que iniciou a verificação de malware contém um arquivo potencialmente malicioso.

Para GuardDuty que a Amazon gere uma descoberta em sua Conta da AWS, ative a Proteção contra Malware GuardDuty e a Proteção contra Malware para S3. A melhor prática é primeiro ativar GuardDuty e depois a Proteção contra Malware para o S3. Se esse pedido for diferente para você, certifique-se de habilitar GuardDuty antes que um objeto do S3 seja carregado em seu bucket protegido.

> **Note**
>
> GuardDuty não é possível gerar uma descoberta para um objeto do S3 que foi escaneado antes da ativação. GuardDuty Para verificar um objeto do S3 em vigor, é possível carregá-lo novamente.

Object:S3/MaliciousFile

Um arquivo malicioso foi detectado em um objeto do S3 verificado.

Gravidade padrão: alta

- Atributo: Proteção contra malware para o S3

Essa descoberta indica que uma verificação de malware detectou que o objeto do S3 listado é malicioso. Para obter mais informações, consulte a seção Ameaças detectadas no painel de detalhes das descobertas.

Recomendações de correção:

Caso essa descoberta seja inesperada, é possível que o objeto do S3 seja malicioso. Para obter informações sobre as etapas de remediação recomendadas, consulte Como corrigir um objeto do S3 possivelmente malicioso.

Proteção contra malware para tipos de descoberta de Backup

GuardDuty O Malware Protection for Backup fornece uma única descoberta para todas as ameaças detectadas durante a verificação do recurso solicitado. A descoberta inclui o número total de detecções feitas durante a verificação e fornece detalhes das 32 principais ameaças detectadas com base na gravidade. Diferentemente de outras GuardDuty descobertas, as descobertas do Malware Protection for Backup não são atualizadas quando o mesmo recurso é examinado novamente. Uma nova descoberta do Malware Protection for Backup é gerada para cada escaneamento que detecta malware.

As descobertas a seguir são específicas do GuardDuty Malware Protection for Backup.

Tópicos

- Execution:EC2/MaliciousFile!Snapshot
- Execution:EC2/MaliciousFile!AMI
- Execution:EC2/MaliciousFile!RecoveryPoint
- Execution:S3/MaliciousFile!RecoveryPoint

Execution:EC2/MaliciousFile!Snapshot

Um arquivo malicioso foi detectado em um snapshot do EBS.

Gravidade padrão: varia de acordo com a ameaça detectada.

- Funcionalidade: Proteção contra malware para backup

Essa descoberta indica que uma verificação do GuardDuty Malware Protection for Backup detectou um ou mais arquivos maliciosos em um snapshot do EBS em seu ambiente. Para obter mais informações, consulte a seção Ameaças detectadas no painel de detalhes das descobertas.

Recomendações de correção:

Se isso for inesperado, o snapshot pode estar comprometido. Para obter mais informações, consulte Corrigindo um snapshot do EBS potencialmente comprometido.

Execution:EC2/MaliciousFile!AMI

Um arquivo mal-intencionado foi detectado em uma AMI do EC2.

Gravidade padrão: varia de acordo com a ameaça detectada.

- Funcionalidade: Proteção contra malware para backup

Essa descoberta indica que uma verificação do GuardDuty Malware Protection for Backup detectou um ou mais arquivos maliciosos em uma AMI em seu ambiente. Para obter mais informações, consulte a seção Ameaças detectadas no painel de detalhes das descobertas.

Recomendações de correção:

Se isso for inesperado, a AMI pode estar comprometida. Para obter mais informações, consulte Corrigindo uma AMI do EC2 potencialmente comprometida.

Execution:EC2/MaliciousFile!RecoveryPoint

Um arquivo malicioso foi detectado em um ponto de recuperação AWS do Backup EC2.

Gravidade padrão: varia de acordo com a ameaça detectada.

- Funcionalidade: Proteção contra malware para backup

Essa descoberta indica que uma verificação do GuardDuty Malware Protection for Backup detectou um ou mais arquivos maliciosos em um ponto de recuperação do EC2 em seu ambiente. O ponto de recuperação afetado pode ser um snapshot do EBS ou uma AMI do EC2. Para obter mais informações, consulte a seção Ameaças detectadas no painel de detalhes das descobertas.

Recomendações de correção:

Se isso for inesperado, o ponto de recuperação do EC2 pode estar comprometido. Para obter mais informações, consulte Corrigindo um ponto de recuperação EC2 potencialmente comprometido.

Execution:S3/MaliciousFile!RecoveryPoint

Um arquivo malicioso foi detectado em um ponto de recuperação AWS do Backup S3.

Gravidade padrão: varia de acordo com a ameaça detectada.

- Funcionalidade: Proteção contra malware para backup

Essa descoberta indica que uma verificação do GuardDuty Malware Protection for Backup detectou um ou mais objetos maliciosos em um ponto de recuperação S3 em seu ambiente. Para obter mais informações, consulte a seção Ameaças detectadas no painel de detalhes das descobertas.

Recomendações de correção:

Se isso for inesperado, o ponto de recuperação do S3 pode estar comprometido. Para obter mais informações, consulte Corrigindo um ponto de recuperação S3 potencialmente comprometido.

GuardDuty Tipos de descoberta do RDS Protection

GuardDuty O RDS Protection detecta um comportamento anômalo de login em sua instância de banco de dados. As descobertas a seguir são específicas do Bancos de dados do Amazon Aurora, Amazon RDS e Aurora Limitless Databases compatíveis e terão um Tipo de recurso de `RDSDBInstance` ou `RDSLimitlessDB`. A gravidade e os detalhes das descobertas serão diferentes com base no tipo de descoberta.

Tópicos

- CredentialAccess:RDS/AnomalousBehavior.SuccessfulLogin
- CredentialAccess:RDS/AnomalousBehavior.FailedLogin
- CredentialAccess:RDS/AnomalousBehavior.SuccessfulBruteForce
- CredentialAccess:RDS/MaliciousIPCaller.SuccessfulLogin
- CredentialAccess:RDS/MaliciousIPCaller.FailedLogin
- Discovery:RDS/MaliciousIPCaller
- CredentialAccess:RDS/TorIPCaller.SuccessfulLogin

- CredentialAccess:RDS/TorIPCaller.FailedLogin
- Discovery:RDS/TorIPCaller
- Exfiltration:RDS/AnomalousBehavior
- Impact:RDS/AnomalousBehavior.Drop
- Impact:RDS/AnomalousBehavior.Delete
- Exfiltration:RDS/MaliciousIPCaller
- Exfiltration:RDS/TorIPCaller
- Impact:RDS/MaliciousIPCaller
- Impact:RDS/TorIPCaller

CredentialAccess:RDS/AnomalousBehavior.SuccessfulLogin

Um usuário fez login com êxito em um banco de dados do RDS em sua conta de forma anômala.

Gravidade padrão: variável

> **Note**
>
> Dependendo do comportamento anômalo associado a essa descoberta, a gravidade padrão pode ser Baixa, Média e Alta.
>
> - Baixa: se o nome de usuário associado a essa descoberta se conectou de um endereço IP associado a uma rede privada.
> - Média: se o nome de usuário associado a essa descoberta se conectou de um endereço IP público.
> - Alto: se houver um padrão consistente de tentativas de login malsucedidas a partir de endereços IP públicos, indicativo de políticas de acesso excessivamente permissivas.

- Atributo: monitoramento de atividade de login do RDS

Essa descoberta informa que um login bem-sucedido anômalo foi observado em um banco de dados do RDS em seu ambiente. AWS Isso pode indicar que um usuário não visto anteriormente fez login em um banco de dados do RDS pela primeira vez. Um cenário comum é um usuário interno fazendo

login em um banco de dados que é acessado programaticamente por aplicativas e não por usuários individuais.

Esse login bem-sucedido foi identificado como anômalo pelo modelo de aprendizado de máquina (ML) de detecção de GuardDuty anomalias. O modelo de ML avalia todos os eventos de login de banco de dados em seus Bancos de dados do Amazon Aurora, Amazon RDS e Aurora Limitless Databases compatíveis e identifica eventos anômalos associados às técnicas usadas pelos adversários. O modelo ML rastreia vários fatores da atividade de login do RDS, como o usuário que fez a solicitação, o local de onde a solicitação foi feita e os detalhes específicos da conexão do banco de dados que foram usados. Para obter informações sobre eventos de login que são potencialmente incomuns, consulte Anomalias baseadas na atividade de login do RDS.

Recomendações de correção:

Se essa atividade for inesperada para o banco de dados associado, é recomendável alterar a senha do usuário do banco de dados associado e revisar os registros de auditoria disponíveis para a atividade realizada pelo usuário anômalo. Descobertas de gravidade média e alta podem indicar que há uma política de acesso ao banco de dados excessivamente permissiva e que as credenciais do usuário podem ter sido expostas ou comprometidas. É recomendável colocar o banco de dados em uma VPC privada e limitar as regras do grupo de segurança para permitir tráfego somente das fontes necessárias. Para obter mais informações, consulte Corrigir um banco de dados potencialmente comprometido com eventos de login bem-sucedidos.

CredentialAccess:RDS/AnomalousBehavior.FailedLogin

Uma ou mais tentativas incomuns de login malsucedidas foram observadas em um banco de dados do RDS em sua conta.

Gravidade padrão: baixa

- Atributo: monitoramento de atividade de login do RDS

Essa descoberta informa que um ou mais logins com falha anômala foram observados em um banco de dados do RDS em seu ambiente. AWS Uma tentativa malsucedida de login de endereços IP públicos pode indicar que o banco de dados do RDS em sua conta foi sujeito a uma tentativa de ataque de força bruta por um agente potencialmente mal-intencionado.

Esses logins com falha foram identificados como anômalos pelo modelo de aprendizado de máquina (ML) de detecção de GuardDuty anomalias. O modelo de ML avalia todos os eventos de login de

banco de dados em seus Bancos de dados do Amazon Aurora, Amazon RDS e Aurora Limitless Databases compatíveis e identifica eventos anômalos associados às técnicas usadas pelos adversários. O modelo ML rastreia vários fatores da atividade de login do RDS, como o usuário que fez a solicitação, o local de onde a solicitação foi feita e os detalhes específicos da conexão do banco de dados que foram usados. Para obter informações sobre as atividades de login do RDS que são potencialmente incomuns, consulte Anomalias baseadas na atividade de login do RDS.

Recomendações de correção:

Se essa atividade for inesperada para o banco de dados associado, isso pode indicar que o banco de dados está exposto publicamente ou que há uma política de acesso excessivamente permissiva ao banco de dados. É recomendável colocar o banco de dados em uma VPC privada e limitar as regras do grupo de segurança para permitir tráfego somente das fontes necessárias. Para obter mais informações, consulte Corrigindo um banco de dados potencialmente comprometido com eventos de login falhados.

CredentialAccess:RDS/AnomalousBehavior.SuccessfulBruteForce

Um usuário fez login com sucesso em um banco de dados do RDS em sua conta a partir de um endereço IP público de forma anômala após um padrão consistente de tentativas incomuns de login malsucedidas.

Gravidade padrão: alta

- Atributo: monitoramento de atividade de login do RDS

Essa descoberta informa que um login anômalo indicativo de uma força bruta bem-sucedida foi observado em um banco de dados do RDS em seu ambiente. AWS Antes de um login bem-sucedido anômalo, foi observado um padrão consistente de tentativas incomuns de login malsucedidas. Isso indica que o usuário e a senha associados ao banco de dados do RDS em sua conta podem ter sido comprometidos e o banco de dados do RDS pode ter sido acessado por um agente potencialmente mal-intencionado.

Esse login bem-sucedido de força bruta foi identificado como anômalo pelo modelo de aprendizado de máquina (ML) de detecção de GuardDuty anomalias. O modelo de ML avalia todos os eventos de login de banco de dados em seus Bancos de dados do Amazon Aurora, Amazon RDS e Aurora Limitless Databases compatíveis e identifica eventos anômalos associados às técnicas usadas pelos adversários. O modelo ML rastreia vários fatores da atividade de login do RDS, como o usuário

que fez a solicitação, o local de onde a solicitação foi feita e os detalhes específicos da conexão do banco de dados que foram usados. Para obter informações sobre as atividades de login do RDS que são potencialmente incomuns, consulte Anomalias baseadas na atividade de login do RDS.

Recomendações de correção:

Essa atividade indica que as credenciais do banco de dados podem ter sido expostas ou comprometidas. É recomendável alterar a senha do usuário do banco de dados associado e revisar os registros de auditoria disponíveis para a atividade realizada pelo usuário potencialmente comprometido. Um padrão consistente de tentativas incomuns de login malsucedidas indica que uma política de acesso excessivamente permissiva ao banco de dados ou o banco de dados também pode ter sido exposto publicamente. É recomendável colocar o banco de dados em uma VPC privada e limitar as regras do grupo de segurança para permitir tráfego somente das fontes necessárias. Para obter mais informações, consulte Corrigir um banco de dados potencialmente comprometido com eventos de login bem-sucedidos.

CredentialAccess:RDS/MaliciousIPCaller.SuccessfulLogin

Um usuário fez login com êxito em um banco de dados do RDS em sua conta de um endereço IP mal-intencionado conhecido.

Gravidade padrão: alta

- Atributo: monitoramento de atividade de login do RDS

Essa descoberta informa que uma atividade bem-sucedida de login do RDS ocorreu a partir de um endereço IP associado a uma atividade maliciosa conhecida em seu AWS ambiente. Isso indica que o usuário e a senha associados ao banco de dados do RDS em sua conta podem ter sido comprometidos e o banco de dados do RDS pode ter sido acessado por um agente potencialmente mal-intencionado.

Recomendações de correção:

Se essa atividade for inesperada para o banco de dados associado, isso pode indicar que as credenciais do usuário podem ter sido expostas ou comprometidas. É recomendável alterar a senha do usuário do banco de dados associado e revisar os registros de auditoria disponíveis para a atividade realizada pelo usuário comprometido. Essa atividade também pode indicar que há uma política de acesso excessivamente permissiva ao banco de dados ou que o banco de dados está exposto publicamente. É recomendável colocar o banco de dados em uma VPC privada e limitar as

regras do grupo de segurança para permitir tráfego somente das fontes necessárias. Para obter mais informações, consulte Corrigir um banco de dados potencialmente comprometido com eventos de login bem-sucedidos.

CredentialAccess:RDS/MaliciousIPCaller.FailedLogin

Um endereço IP associado a uma atividade mal-intencionada conhecida tentou, sem sucesso, fazer login em um banco de dados do RDS em sua conta.

Gravidade padrão: média

- Atributo: monitoramento de atividade de login do RDS

Essa descoberta informa que um endereço IP associado a uma atividade maliciosa conhecida tentou fazer login em um banco de dados do RDS em seu AWS ambiente, mas não forneceu o nome de usuário ou a senha corretos. Isso indica que um agente possivelmente mal-intencionado pode estar tentando comprometer o banco de dados do RDS em sua conta.

Recomendações de correção:

Se essa atividade for inesperada para o banco de dados associado, isso pode indicar que há uma política de acesso excessivamente permissiva ao banco de dados ou que o banco de dados está exposto publicamente. É recomendável colocar o banco de dados em uma VPC privada e limitar as regras do grupo de segurança para permitir tráfego somente das fontes necessárias. Para obter mais informações, consulte Corrigindo um banco de dados potencialmente comprometido com eventos de login falhados.

Discovery:RDS/MaliciousIPCaller

Um endereço IP associado a uma atividade mal-intencionada conhecida investigou um banco de dados do RDS em sua conta; nenhuma tentativa de autenticação foi feita.

Gravidade padrão: média

- Atributo: monitoramento de atividade de login do RDS

Essa descoberta informa que um endereço IP associado a uma atividade maliciosa conhecida investigou um banco de dados do RDS em seu AWS ambiente, embora nenhuma tentativa de login

tenha sido feita. Isso pode indicar que um agente possivelmente mal-intencionado está tentando escanear uma infraestrutura acessível ao público.

Recomendações de correção:

Se essa atividade for inesperada para o banco de dados associado, isso pode indicar que há uma política de acesso excessivamente permissiva ao banco de dados ou que o banco de dados está exposto publicamente. É recomendável colocar o banco de dados em uma VPC privada e limitar as regras do grupo de segurança para permitir tráfego somente das fontes necessárias. Para obter mais informações, consulte Corrigindo um banco de dados potencialmente comprometido com eventos de login falhados.

CredentialAccess:RDS/TorIPCaller.SuccessfulLogin

Um usuário fez login com êxito em um banco de dados do RDS em sua conta de um endereço IP do nó de saída do Tor.

Gravidade padrão: alta

- Atributo: monitoramento de atividade de login do RDS

Essa descoberta informa que um usuário fez login com êxito em um banco de dados do RDS em seu ambiente da AWS usando um endereço IP do nó de saída do Tor. Tor é um software para permitir a comunicação anônima. Ele criptografa e aleatoriamente envia comunicações por meio de relés entre uma série de nós de rede. O último nó do Tor é chamado de nó de saída. Isso pode indicar um acesso não autorizado aos seus recursos do RDS com a intenção de ocultar a verdadeira identidade do usuário anônimo.

Recomendações de correção:

Se essa atividade for inesperada para o banco de dados associado, isso pode indicar que as credenciais do usuário podem ter sido expostas ou comprometidas. É recomendável alterar a senha do usuário do banco de dados associado e revisar os registros de auditoria disponíveis para a atividade realizada pelo usuário comprometido. Essa atividade também pode indicar que há uma política de acesso excessivamente permissiva ao banco de dados ou que o banco de dados está exposto publicamente. É recomendável colocar o banco de dados em uma VPC privada e limitar as regras do grupo de segurança para permitir tráfego somente das fontes necessárias. Para obter mais informações, consulte Corrigir um banco de dados potencialmente comprometido com eventos de login bem-sucedidos.

CredentialAccess:RDS/TorIPCaller.FailedLogin

Um endereço IP do Tor tentou fazer login sem êxito em um banco de dados do RDS em sua conta.

Gravidade padrão: média

- Atributo: monitoramento de atividade de login do RDS

Essa descoberta informa que um endereço IP do nó de saída do Tor tentou fazer login em um banco de dados do RDS em seu AWS ambiente, mas falhou em fornecer o nome de usuário ou a senha corretos. O Tor é um software para permitir a comunicação anônima. Ele criptografa e aleatoriamente envia comunicações por meio de relés entre uma série de nós de rede. O último nó do Tor é chamado de nó de saída. Isso pode indicar um acesso não autorizado aos seus recursos do RDS com a intenção de ocultar a verdadeira identidade do usuário anônimo.

Recomendações de correção:

Se essa atividade for inesperada para o banco de dados associado, isso pode indicar que há uma política de acesso excessivamente permissiva ao banco de dados ou que o banco de dados está exposto publicamente. É recomendável colocar o banco de dados em uma VPC privada e limitar as regras do grupo de segurança para permitir tráfego somente das fontes necessárias. Para obter mais informações, consulte Corrigindo um banco de dados potencialmente comprometido com eventos de login falhados.

Discovery:RDS/TorIPCaller

Um endereço IP do nó de saída do Tor investigou um banco de dados RDS em sua conta, nenhuma tentativa de autenticação foi feita.

Gravidade padrão: média

- Atributo: monitoramento de atividade de login do RDS

Essa descoberta informa que um endereço IP do nó de saída do Tor sondou um banco de dados RDS em seu ambiente da AWS , embora nenhuma tentativa de login tenha sido feita. Isso pode indicar que um agente potencialmente mal-intencionado está tentando escanear a infraestrutura acessível ao público. Tor é um software para permitir a comunicação anônima. Ele criptografa e

aleatoriamente envia comunicações por meio de retransmissões entre uma série de nós de rede. O último nó do Tor é chamado de nó de saída. Isso pode indicar um acesso não autorizado aos recursos do RDS em sua conta com a intenção de ocultar a verdadeira identidade do invasor potencialmente nocivo.

Recomendações de correção:

Se essa atividade for inesperada para o banco de dados associado, isso pode indicar que há uma política de acesso excessivamente permissiva ao banco de dados ou que o banco de dados está exposto publicamente. É recomendável colocar o banco de dados em uma VPC privada e limitar as regras do grupo de segurança para permitir tráfego somente das fontes necessárias. Para obter mais informações, consulte Corrigindo um banco de dados potencialmente comprometido com eventos de login falhados.

Exfiltration:RDS/AnomalousBehavior

Atividade anômala de um usuário que extrai grande volume de dados de um banco de dados do RDS em sua conta.

Gravidade padrão: baixa

> **Note**
>
> Dependendo do comportamento anômalo associado a essa descoberta, a severidade padrão pode ser Baixa, Média ou Alta.
>
> - Baixo — Se o nome de usuário associado a essa descoberta executou `SELECT` instruções de um endereço IP associado a uma rede privada.
> - Médio — Se o nome de usuário associado a essa descoberta executou `SELECT` instruções de um endereço IP público.
> - Alto — Se o nome de usuário associado a essa descoberta executou `SELECT` instruções retornando um volume invulgarmente grande de linhas e a atividade se originou de uma rede pública nunca vista anteriormente ou foi executada por uma função de banco de dados ou cliente administrativo de alto privilégio.

- Funcionalidade: Monitoramento de atividades do banco de dados RDS

Essa descoberta informa que uma atividade anômala do banco de dados consistente com a exfiltração de dados foi observada em um banco de dados do RDS em seu ambiente. AWS Isso pode indicar que um usuário do banco de dados selecionou um número significativamente maior de linhas do que o normal ou que a atividade envolveu um atributo de banco de dados inédito, como um novo usuário, endereço IP ou nome de banco de dados que contribuiu para o aumento do volume. Um cenário comum é o uso de uma credencial de banco de dados comprometida para extrair dados por meio de uma combinação de padrões de acesso incomuns e volume elevado de consultas.

Essa atividade foi identificada como anômala pelo modelo de aprendizado de máquina (ML) de detecção de GuardDuty anomalias. O modelo de ML avalia todos os eventos de atividade do banco de dados em seu Bancos de dados do Amazon Aurora, Amazon RDS e Aurora Limitless Databases compatíveis e identifica eventos anômalos associados às técnicas usadas pelos adversários. O modelo ML rastreia vários fatores da atividade do banco de dados do RDS, como o usuário que fez a solicitação, as consultas executadas, o volume de dados acessados e os detalhes específicos da conexão do banco de dados que foram usados. Para obter informações sobre a atividade do banco de dados que é potencialmente incomum, consulteAnomalias baseadas em atividades de dados do RDS.

Recomendações de correção:

Se essa atividade for inesperada para o banco de dados associado, é recomendável alterar a senha do usuário do banco de dados associado e revisar os registros de auditoria disponíveis para determinar quais dados o usuário anômalo acessou. É recomendável colocar o banco de dados em uma VPC privada e limitar as regras do grupo de segurança para permitir tráfego somente das fontes necessárias. Para obter mais informações, consulte Corrigindo um banco de dados potencialmente comprometido com atividade de exfiltração anômala.

Impact:RDS/AnomalousBehavior.Drop

Atividade anômala de um usuário que remove dados de um banco de dados do RDS em sua conta.

Gravidade padrão: média

> **Note**
>
> Dependendo do comportamento anômalo associado a essa descoberta, a severidade padrão pode ser Média ou Alta.

- Médio — Se o nome de usuário associado a essa descoberta executou declarações anômalasDROP.
- Alto — Se o nome de usuário associado a essa descoberta executou várias DROP instruções e a atividade se originou de uma rede pública inédita ou foi executada por uma função de banco de dados ou cliente administrativo de alto privilégio.

- Funcionalidade: Monitoramento de atividades do banco de dados RDS

Essa descoberta informa que uma atividade anômala do banco de dados consistente com operações destrutivas foi observada em um banco de dados do RDS em seu ambiente. AWS Isso pode indicar que um usuário do banco de dados eliminou um número significativamente maior de tabelas ou objetos do banco de dados do que o normal, ou que a atividade envolveu um atributo de banco de dados inédito, como um novo usuário, endereço IP ou nome de aplicativo que contribuiu para a operação destrutiva. Um cenário comum é uma credencial de banco de dados comprometida sendo usada para destruir estruturas de banco de dados por meio de uma combinação de padrões de acesso incomuns e volume elevado de DROP declarações.

Essa atividade foi identificada como anômala pelo modelo de aprendizado de máquina (ML) de detecção de GuardDuty anomalias. O modelo de ML avalia todos os eventos de atividade do banco de dados em seu Bancos de dados do Amazon Aurora, Amazon RDS e Aurora Limitless Databases compatíveis e identifica eventos anômalos associados às técnicas usadas pelos adversários. O modelo ML rastreia vários fatores da atividade do banco de dados do RDS, como o usuário que fez a solicitação, as instruções executadas, os objetos do banco de dados direcionados e os detalhes específicos da conexão do banco de dados que foram usados. Para obter informações sobre a atividade do banco de dados que é potencialmente incomum, consulteAnomalias baseadas em atividades de dados do RDS.

Recomendações de correção:

Se essa atividade for inesperada para o banco de dados associado, é recomendável alterar imediatamente a senha do usuário do banco de dados associado e revogar seu acesso. Analise os registros de auditoria disponíveis para determinar o escopo dos objetos descartados e inicie a recuperação dos backups, se necessário. Também é recomendável colocar o banco de dados em uma VPC privada e limitar as regras do grupo de segurança para permitir tráfego somente das fontes necessárias. Para obter mais informações, consulte Corrigindo um banco de dados potencialmente comprometido com atividade destrutiva anômala.

Impact:RDS/AnomalousBehavior.Delete

Atividade anômala de um usuário excluindo dados de um banco de dados do RDS em sua conta.

Gravidade padrão: baixa

> **Note**
>
> Dependendo do comportamento anômalo associado a essa descoberta, a severidade padrão pode ser Baixa, Média ou Alta.
>
> - Baixo — Se o nome de usuário associado a essa descoberta executou `DELETE` instruções de um endereço IP associado a uma rede privada.
> - Médio — Se o nome de usuário associado a essa descoberta executou `DELETE` instruções de um endereço IP público.
> - Alto — Se o nome de usuário associado a essa descoberta executou `DELETE` instruções retornando um volume invulgarmente grande de linhas e a atividade se originou de uma rede pública nunca vista anteriormente ou foi executada por uma função de banco de dados ou cliente administrativo de alto privilégio.

- Funcionalidade: Monitoramento de atividades do banco de dados RDS

Essa descoberta informa que uma atividade anômala do banco de dados consistente com operações destrutivas foi observada em um banco de dados do RDS em seu ambiente. AWS Isso pode indicar que um usuário do banco de dados excluiu um número significativamente maior de linhas do que o normal ou que a atividade envolveu um atributo de banco de dados inédito, como um novo usuário, endereço IP ou nome do aplicativo, que contribuiu para a operação destrutiva. Um cenário comum é o uso de uma credencial de banco de dados comprometida para remover dados sistematicamente por meio de uma combinação de padrões de acesso incomuns e volume elevado `DELETE` de declarações.

Essa atividade foi identificada como anômala pelo modelo de aprendizado de máquina (ML) de detecção de GuardDuty anomalias. O modelo de ML avalia todos os eventos de atividade do banco de dados em seu Bancos de dados do Amazon Aurora, Amazon RDS e Aurora Limitless Databases compatíveis e identifica eventos anômalos associados às técnicas usadas pelos adversários. O

modelo ML rastreia vários fatores da atividade do banco de dados do RDS, como o usuário que fez a solicitação, as instruções executadas, o número de linhas afetadas e os detalhes específicos da conexão do banco de dados que foram usados. Para obter informações sobre a atividade do banco de dados que é potencialmente incomum, consulteAnomalias baseadas em atividades de dados do RDS.

Recomendações de correção:

Se essa atividade for inesperada para o banco de dados associado, é recomendável alterar imediatamente a senha do usuário do banco de dados associado e revogar seu acesso. Analise os registros de auditoria disponíveis para determinar o escopo dos dados excluídos e inicie a recuperação pontual a partir de backups automatizados se a perda de dados for confirmada. Também é recomendável colocar o banco de dados em uma VPC privada e limitar as regras do grupo de segurança para permitir tráfego somente das fontes necessárias. Para obter mais informações, consulte Corrigindo um banco de dados potencialmente comprometido com atividade destrutiva anômala.

Exfiltration:RDS/MaliciousIPCaller

Um endereço IP associado a atividades maliciosas conhecidas executou consultas de extração de dados em um banco de dados do RDS em sua conta.

Gravidade padrão: alta

- Funcionalidade: Monitoramento de atividades do banco de dados RDS

Essa descoberta informa que um endereço IP associado a uma atividade maliciosa conhecida executou consultas de banco de dados consistentes com a exfiltração de dados em um banco de dados RDS em seu ambiente. AWS Isso indica que o usuário e a senha associados ao banco de dados do RDS em sua conta podem ter sido comprometidos, e os dados do banco de dados do RDS podem ter sido extraídos por um agente potencialmente mal-intencionado.

Recomendações de correção:

Se essa atividade for inesperada para o banco de dados associado, isso pode indicar que as credenciais do usuário podem ter sido expostas ou comprometidas. É recomendável alterar a senha do usuário do banco de dados associado e revisar os registros de dados do RDS disponíveis para verificar a atividade realizada pelo usuário comprometido. É recomendável identificar os dados que estavam acessíveis ao usuário afetado e avaliar o impacto comercial de quaisquer dados

potencialmente exfiltrados. Também é recomendável colocar o banco de dados em uma VPC privada e limitar as regras do grupo de segurança para permitir tráfego somente das fontes necessárias. Para obter mais informações, consulte Corrigindo um banco de dados potencialmente comprometido com atividade de exfiltração anômala.

Exfiltration:RDS/TorIPCaller

Um endereço IP do nó de saída do Tor executou consultas de extração de dados em um banco de dados RDS em sua conta.

Gravidade padrão: alta

- Funcionalidade: Monitoramento de atividades do banco de dados RDS

Essa descoberta informa que um endereço IP do nó de saída do Tor executou consultas de banco de dados consistentes com a exfiltração de dados em um banco de dados RDS em seu ambiente. AWS O Tor é um software para permitir a comunicação anônima. Ele criptografa e aleatoriamente envia comunicações por meio de relés entre uma série de nós de rede. O último nó do Tor é chamado de nó de saída. Isso pode indicar acesso não autorizado aos recursos do RDS em sua conta, com a intenção de ocultar a verdadeira identidade do usuário anônimo enquanto extrai dados.

Recomendações de correção:

Se essa atividade for inesperada para o banco de dados associado, isso pode indicar que as credenciais do usuário podem ter sido expostas ou comprometidas. É recomendável alterar a senha do usuário do banco de dados associado e revisar os registros de dados do RDS disponíveis para verificar a atividade realizada pelo usuário comprometido. É recomendável identificar os dados que estavam acessíveis ao usuário afetado e avaliar o impacto comercial de quaisquer dados potencialmente exfiltrados. Também é recomendável colocar o banco de dados em uma VPC privada e limitar as regras do grupo de segurança para permitir tráfego somente das fontes necessárias. Para obter mais informações, consulte Corrigindo um banco de dados potencialmente comprometido com atividade de exfiltração anômala.

Impact:RDS/MaliciousIPCaller

Um endereço IP associado a atividades maliciosas conhecidas executou declarações destrutivas em um banco de dados do RDS em sua conta.

Gravidade padrão: alta

- Funcionalidade: Monitoramento de atividades do banco de dados RDS

Essa descoberta informa que um endereço IP associado a uma atividade maliciosa conhecida executou declarações de banco de dados com impacto destrutivo em um banco de dados RDS em seu ambiente. AWS Isso indica que o usuário e a senha associados ao banco de dados do RDS em sua conta podem ter sido comprometidos, e o banco de dados do RDS pode ter sido submetido a operações destrutivas por um agente potencialmente mal-intencionado.

Recomendações de correção:

Se essa atividade for inesperada para o banco de dados associado, isso pode indicar que as credenciais do usuário podem ter sido expostas ou comprometidas. É recomendável alterar imediatamente a senha do usuário do banco de dados associado e revogar seu acesso. Analise os registros de dados do RDS disponíveis para determinar o escopo das operações destrutivas realizadas e inicie a recuperação dos backups, se necessário. Também é recomendável colocar o banco de dados em uma VPC privada e limitar as regras do grupo de segurança para permitir tráfego somente das fontes necessárias. Para obter mais informações, consulte Corrigindo um banco de dados potencialmente comprometido com atividade destrutiva anômala.

Impact:RDS/TorIPCaller

Um endereço IP do nó de saída do Tor executou declarações destrutivas em um banco de dados RDS em sua conta.

Gravidade padrão: alta

- Funcionalidade: Monitoramento de atividades do banco de dados RDS

Essa descoberta informa que um endereço IP do nó de saída do Tor executou declarações de banco de dados com impacto destrutivo em um banco de dados RDS em seu ambiente. AWS O Tor é uma rede de sobreposição para permitir a comunicação anônima. Ele criptografa e aleatoriamente envia comunicações por meio de relés entre uma série de nós de rede. O último nó do Tor é chamado de nó de saída. Isso pode indicar acesso não autorizado aos recursos do RDS em sua conta, com a intenção de ocultar a verdadeira identidade do usuário anônimo enquanto executa operações destrutivas.

Recomendações de correção:

Se essa atividade for inesperada para o banco de dados associado, isso pode indicar que as credenciais do usuário podem ter sido expostas ou comprometidas. É recomendável alterar imediatamente a senha do usuário do banco de dados associado e revogar seu acesso. Analise os registros de dados do RDS disponíveis para determinar o escopo das operações destrutivas realizadas e inicie a recuperação dos backups, se necessário. Também é recomendável colocar o banco de dados em uma VPC privada e limitar as regras do grupo de segurança para permitir tráfego somente das fontes necessárias. Para obter mais informações, consulte Corrigindo um banco de dados potencialmente comprometido com atividade destrutiva anômala.

Tipos de descoberta da Proteção do Lambda

Esta seção descreve os tipos de descoberta que são específicos de seus AWS Lambda recursos e estão `resourceType` listados como`Lambda`. Para todas as descobertas do Lambda, recomendamos que você examine o recurso em questão e determine se ele está se comportando da maneira esperada. Se a atividade for autorizada, você poderá usar regras de supressão ou listas de IPs confiáveis e de ameaças para evitar notificações de falsos positivos para esse recurso.

Se a atividade for inesperada, a melhor prática de segurança é presumir que o Lambda foi potencialmente comprometido e seguir as recomendações de remediação.

Tópicos

- Backdoor:Lambda/C&CActivity.B
- CryptoCurrency:Lambda/BitcoinTool.B
- Trojan:Lambda/BlackholeTraffic
- Trojan:Lambda/DropPoint
- UnauthorizedAccess:Lambda/MaliciousIPCaller.Custom
- UnauthorizedAccess:Lambda/TorClient
- UnauthorizedAccess:Lambda/TorRelay

Backdoor:Lambda/C&CActivity.B

Uma função do Lambda está consultando um endereço IP associado a um servidor de comando e controle conhecido.

Gravidade padrão: alta

- Atributo: Monitoramento de atividades de rede do Lambda

Essa descoberta informa que uma função Lambda listada em AWS seu ambiente está consultando um endereço IP associado a um servidor de comando e controle (C&C) conhecido. A função do Lambda associada à descoberta gerada está potencialmente comprometida. Os servidores C&C são computadores que enviam comandos para membros de um botnet.

Um botnet é uma coleção de dispositivos conectados à Internet (que podem incluir PCs, servidores, dispositivos móveis e dispositivos de Internet das Coisas) infectados e controlados por um tipo comum de malware. Os botnets são frequentemente usados para distribuir malwares e coletar informações inapropriadas, como números de cartão de crédito. Dependendo da finalidade e da estrutura do botnet, o servidor C&C também pode emitir comandos para iniciar um ataque de negação distribuída de serviço DDoS.

Recomendações de correção:

Se essa atividade for inesperada, sua função do Lambda pode estar comprometida. Para obter mais informações, consulte Correção de uma função do Lambda comprometida.

CryptoCurrency:Lambda/BitcoinTool.B

Uma função do Lambda está consultando um endereço IP associado à atividade relacionada a uma criptomoeda.

Gravidade padrão: alta

- Atributo: Monitoramento de atividades de rede do Lambda

Essa descoberta informa que a função Lambda listada em AWS seu ambiente está consultando um endereço IP associado a um Bitcoin ou outra atividade relacionada à criptomoeda. Os agentes de ameaças podem tentar assumir o controle das funções do Lambda para redirecioná-las de maneira mal-intencionada para a mineração não autorizada de criptomoedas.

Recomendações de correção:

Se você usa essa função do Lambda para minerar ou gerenciar criptomoedas, ou se essa função estiver envolvida em uma atividade de blockchain, ela é potencialmente uma atividade esperada para seu ambiente. Se esse for o caso em seu AWS ambiente, recomendamos que você configure

uma regra de supressão para essa descoberta. A regra de supressão deve consistir em dois critérios de filtro. O primeiro critério deve usar o atributo Tipo de descoberta com um valor de CryptoCurrency:Lambda/BitcoinTool.B. O segundo critério de filtro deve ser o nome da função do Lambda da função envolvida na atividade do blockchain. Para obter informações sobre a criação de regras de supressão, consulte Regras de supressão.

Se essa atividade for inesperada, sua função do Lambda está potencialmente comprometida. Para obter mais informações, consulte Correção de uma função do Lambda comprometida.

Trojan:Lambda/BlackholeTraffic

A função do Lambda está tentando se comunicar com um endereço IP de um host remoto que é um buraco negro conhecido.

Gravidade padrão: média

- Atributo: Monitoramento de atividades de rede do Lambda

Essa descoberta informa que uma função Lambda listada em AWS seu ambiente está tentando se comunicar com o endereço IP de um buraco negro (ou sumidouro). Buracos negros são lugares na rede em que o tráfego de entrada ou saída é descartado silenciosamente sem informar à fonte que os dados não chegaram ao destinatário pretendido. Um endereço IP de buraco negro especifica uma máquina host que não está sendo executada ou um endereço para o qual nenhum host foi atribuído. A função do Lambda listada está potencialmente comprometida.

Recomendações de correção:

Se essa atividade for inesperada, sua função do Lambda pode estar comprometida. Para obter mais informações, consulte Correção de uma função do Lambda comprometida.

Trojan:Lambda/DropPoint

Uma função do Lambda está tentando se comunicar com um endereço IP de um host remoto que é conhecido por manter credenciais e outros dados roubados capturados por malware.

Gravidade padrão: média

- Atributo: Monitoramento de atividades de rede do Lambda

Essa descoberta informa que uma função Lambda listada em AWS seu ambiente está tentando se comunicar com um endereço IP de um host remoto que é conhecido por conter credenciais e outros dados roubados capturados por malware.

Recomendações de correção:

Se essa atividade for inesperada, sua função do Lambda pode estar comprometida. Para obter mais informações, consulte Correção de uma função do Lambda comprometida.

UnauthorizedAccess:Lambda/MaliciousIPCaller.Custom

Uma função do Lambda está fazendo conexões com um endereço IP em uma lista de ameaças personalizada.

Gravidade padrão: média

- Atributo: Monitoramento de atividades de rede do Lambda

Essa descoberta informa que uma função Lambda em AWS seu ambiente está se comunicando com um endereço IP incluído em uma lista de ameaças que você enviou. Em GuardDuty, uma lista de ameaças consiste em endereços IP maliciosos conhecidos. GuardDuty gera descobertas com base nas listas de ameaças enviadas. Você pode ver os detalhes da lista de ameaças nos detalhes da descoberta no GuardDuty console.

Recomendações de correção:

Se essa atividade for inesperada, sua função do Lambda pode estar comprometida. Para obter mais informações, consulte Correção de uma função do Lambda comprometida.

UnauthorizedAccess:Lambda/TorClient

A função do Lambda está fazendo conexões com um Tor Guard ou um nó de autoridade.

Gravidade padrão: alta

- Atributo: Monitoramento de atividades de rede do Lambda

Essa descoberta informa que uma função Lambda em AWS seu ambiente está fazendo conexões com um Tor Guard ou um nó de Autoridade. Tor é um software para permitir a comunicação

anônima. Tor Guards ou nós de autoridade atuam como gateways iniciais em uma rede do Tor. Esse tráfego pode indicar que essa função do Lambda foi potencialmente comprometida. Agora ele está atuando como um cliente em uma rede Tor.

Recomendações de correção:

Se essa atividade for inesperada, sua função do Lambda pode estar comprometida. Para obter mais informações, consulte Correção de uma função do Lambda comprometida.

UnauthorizedAccess:Lambda/TorRelay

Uma função do Lambda está fazendo conexões com uma rede Tor como uma retransmissão Tor.

Gravidade padrão: alta

- Atributo: Monitoramento de atividades de rede do Lambda

Essa descoberta informa que uma função Lambda em AWS seu ambiente está fazendo conexões com uma rede Tor de uma maneira que sugere que ela está agindo como um retransmissor Tor. Tor é um software para permitir a comunicação anônima. O Tor habilita a comunicação anônima encaminhando tráfego potencialmente ilícito do cliente de uma retransmissão Tor para outra.

Recomendações de correção:

Se essa atividade for inesperada, sua função do Lambda pode estar comprometida. Para obter mais informações, consulte Correção de uma função do Lambda comprometida.

GuardDuty Tipos de descoberta de proteção de IA

Quando você ativa o AI Protection, GuardDuty analisa eventos AWS CloudTrail de gerenciamento e eventos de dados do Amazon Bedrock e do Amazon SageMaker AI. GuardDuty usa esses dados para detectar atividades potencialmente suspeitas que tenham como alvo suas cargas de trabalho de IA. Quando GuardDuty detecta uma ameaça em potencial, ele gera um dos seguintes tipos de descoberta. O `Resource type` valor dessas descobertas é`AccessKey`, e a descoberta identifica a identidade do IAM que invocou o modelo.

Cada descoberta também inclui detalhes sobre os recursos de IA afetados no `resource` objeto da descoberta. Impact:IAMUser/CostHarvestingAs descobertas Impact:IAMUser/

AnomalousModelInvocation e incluem uma `resource.modelDetails` lista que identifica os modelos invocados do Amazon Bedrock ou da Amazon SageMaker AI. A Impact:IAMUser/PromptInjection.Direct descoberta inclui um `resource.bedrockGuardrailDetails` objeto que descreve o Amazon Bedrock Guardrail que interveio. Você pode ver esses detalhes no GuardDuty console ou no JSON de localização.

Os tipos de Impact:IAMUser/CostHarvesting descoberta Impact:IAMUser/AnomalousModelInvocation e descoberta se aplicam às invocações de modelos Amazon Bedrock e Amazon SageMaker AI. O tipo de Impact:IAMUser/PromptInjection.Direct descoberta se aplica às cargas de trabalho do Amazon Bedrock que usam o Amazon Bedrock Guardrails.

Tópicos

- Impact:IAMUser/AnomalousModelInvocation
- Impact:IAMUser/CostHarvesting
- Impact:IAMUser/PromptInjection.Direct

Impact:IAMUser/AnomalousModelInvocation

Uma identidade do IAM invocou um modelo Amazon Bedrock ou Amazon SageMaker AI de uma forma que se desvia da linha de base estabelecida para a identidade ou conta.

Gravidade padrão: baixa

- Característica: Proteção AI

Essa descoberta informa que uma identidade do IAM invocou um modelo Amazon Bedrock ou Amazon SageMaker AI de uma forma que se desvia da atividade histórica da identidade ou da conta. Essa atividade pode indicar que um agente de ameaças está usando credenciais comprometidas para acessar modelos básicos em sua conta. Por exemplo, o ator pode sondar um modelo, criar entradas adversárias ou executar solicitações automatizadas.

GuardDuty estabelece uma linha de base da atividade normal de invocação do modelo para cada identidade do IAM e invoca o Amazon Conta da AWS Bedrock ou o Amazon AI. SageMaker GuardDuty traça perfis de características da atividade de invocação, incluindo o seguinte:

- A API de invocação do modelo que a identidade chamou

- O modelo que a identidade invocou
- O endereço IP de origem e sua organização associada ao Número de Sistema Autônomo (ASN)
- O agente do usuário que fez a solicitação

Quando GuardDuty observa uma atividade que se desvia significativamente dessa linha de base, gera esse achado. Os exemplos incluem invocações de um endereço IP inédito, de um agente de usuário inédito ou de um modelo que a identidade nunca invocou. A descoberta inclui uma `resource.modelDetails` lista que identifica os modelos envolvidos na atividade suspeita. Cada entrada contém uma `modelId` representação de um modelo básico do Amazon Bedrock, perfil de inferência, modelo ARN provisionado, personalizado ou importado, endpoint do Amazon Bedrock Marketplace, recurso de solicitação ou nome do endpoint Amazon AI. SageMaker

Essa descoberta está vinculada à técnica MITRE ATLAS AML.T0040 - AI Model Inference API Access no site MITRE ATLAS.

Recomendações de correção:

Se essa atividade for inesperada, suas credenciais podem estar comprometidas. Para obter mais informações, consulte Correção de problemas potencialmente comprometidos AWS credenciais.

Para reduzir o risco de invocações de modelos não autorizadas, restrinja quais identidades podem invocar modelos. Estabeleça o acesso às seguintes APIs de invocação de modelo somente para os diretores e modelos que as exigem:

- `bedrock:InvokeModel`
- `bedrock:InvokeModelWithResponseStream`
- `bedrock:Converse`
- `bedrock:ConverseStream`
- `bedrock-mantle:CreateInference`
- `sagemaker:InvokeEndpoint`
- `sagemaker:InvokeEndpointAsync`
- `sagemaker:InvokeEndpointWithResponseStream`

Para negar a inferência de modelos em sua organização onde ela não é necessária, você pode usar uma política de controle de serviços (SCP). Para obter mais informações, consulte exemplos de Identity-based políticas para o Amazon Bedrock no Guia do usuário do Amazon

Bedrock e exemplos de políticas baseadas em identidade do Amazon SageMaker AI no Guia do desenvolvedor do Amazon SageMaker AI.

Impact:IAMUser/CostHarvesting

Uma identidade do IAM invocou um modelo Amazon Bedrock ou Amazon SageMaker AI com volumes de tokens anômalos que podem indicar um ataque de coleta de custos.

Gravidade padrão: baixa

- Característica: Proteção AI

Essa descoberta informa que uma identidade do IAM invocou um modelo Amazon Bedrock ou Amazon SageMaker AI com volumes de token de entrada ou saída que se desviam significativamente da linha de base da identidade ou da conta. Em um ataque de coleta de custos, um agente de ameaça envia entradas computacionalmente caras para um modelo para aumentar os custos operacionais da workload de IA, sem necessariamente exfiltrar dados. Essas entradas podem incluir prompts excessivamente longos ou deliberadamente malformados.

GuardDuty estabelece uma linha de base do volume médio do token de entrada e do volume médio do token de saída para cada identidade e conta do IAM que invoca os modelos Amazon Bedrock ou Amazon AI. SageMaker Quando GuardDuty observa invocações com contagens de tokens que excedem essa linha de base e correlaciona a anomalia de volume com outros sinais incomuns, gera essa descoberta. GuardDuty A descoberta relata a atividade anômala no `service.detection` objeto, incluindo a invocação observada e os volumes de tokens que se desviaram da linha de base. Também inclui uma `resource.modelDetails` lista que identifica os modelos alvo. Cada entrada contém uma `modelId` representação de um modelo básico do Amazon Bedrock, perfil de inferência, modelo ARN provisionado, personalizado ou importado, endpoint do Amazon Bedrock Marketplace, recurso de solicitação ou nome do endpoint Amazon AI. SageMaker

Essa descoberta corresponde à técnica MITRE ATLAS AML.T0034 - Cost Harvesting no site MITRE ATLAS.

Recomendações de correção:

Se essa atividade for inesperada para a identidade associada, as credenciais podem ter sido comprometidas e usadas para aumentar o custo de suas cargas de trabalho de IA. Para obter mais

informações, consulte Correção de problemas potencialmente comprometidos AWS credenciais. Analise as invocações de modelo associadas à identidade e restrinja o acesso aos modelos afetados definindo o escopo do acesso às seguintes APIs de invocação de modelo somente para os principais que as exigem:

- `bedrock:InvokeModel`
- `bedrock:InvokeModelWithResponseStream`
- `bedrock:Converse`
- `bedrock:ConverseStream`
- `bedrock-mantle:CreateInference`
- `sagemaker:InvokeEndpoint`
- `sagemaker:InvokeEndpointAsync`
- `sagemaker:InvokeEndpointWithResponseStream`

Para detectar e conter gastos anormais, você pode usar orçamentos, incluindo ações AWS orçamentárias que aplicam uma política de IAM restritiva quando um limite de orçamento é excedido e a detecção de anomalias de custo. AWS Para atribuir os custos do Amazon Bedrock a cargas de trabalho específicas, você pode anexar etiquetas de alocação de custos a um perfil de inferência do aplicativo.

Impact:IAMUser/PromptInjection.Direct

Uma barreira de proteção do Amazon Bedrock detectou uma tentativa direta de injeção de prompt em uma invocação feita por uma identidade do IAM.

Gravidade padrão: baixa

- Característica: Proteção AI

Essa descoberta informa que uma barreira de proteção do Amazon Bedrock configurada para uma workload do Amazon Bedrock em sua conta detectou uma tentativa direta de injeção de prompt. Em um ataque de injeção direta, um agente de ameaças cria um aviso malicioso como entrada para um modelo básico. O aviso faz com que o modelo ignore suas instruções originais e, em vez disso, siga as instruções do atacante. A injeção de prompt pode dar ao invasor acesso inicial para realizar etapas adicionais contra um aplicativo de IA, como exfiltrar dados, chamar ferramentas não autorizadas ou contornar controles de segurança.

GuardDuty gera essa descoberta quando um Amazon Bedrock Guardrail intervém em uma invocação porque detectou um ataque imediato com alta confiança. Para permitir GuardDuty a detecção de injeção direta, configure um Amazon Bedrock Guardrail com um filtro de conteúdo de ataque imediato. Para garantir que a grade de proteção avalie as invocações em todo o seu ambiente, aplique-a amplamente, em vez de depender de aplicativos individuais para anexá-la a cada solicitação. Você pode aplicar uma barreira para todas as invocações do modelo Amazon Bedrock em uma conta ou em toda a sua organização usando as políticas do Amazon Bedrock em. AWS Organizations Para obter mais informações, consulte Aplicar salvaguardas entre contas com as imposições do Amazon Bedrock Guardrails no Guia do usuário do Amazon Bedrock. Quando um guardrail avalia uma invocação, o Amazon Bedrock registra a avaliação em eventos de AWS CloudTrail dados, que GuardDuty são analisados para gerar essa descoberta. Se o guardrail também aplicou um filtro de informações confidenciais ao avaliar a invocação, a descoberta incluirá detalhes sobre o tipo de informação confidencial detectada.

A descoberta inclui um objeto `resource.bedrockGuardrailDetails` que descreve a barreira de proteção que interveio. A tabela a seguir descreve os campos desse objeto.

Campo	Description
`guardrails`	Uma lista das barreiras que avaliaram a invocação. Cada entrada inclui o nome de recurso da Amazon (`arn`) e o `version` da grade de proteção. Várias grades de proteção podem aparecer quando uma grade de proteção aplicada pela conta ou pela organização e uma grade de proteção em nível de solicitação avaliam a mesma invocação.
`guardrailAction`	A ação que o guardrail realizou. GuardDuty gera essa descoberta quando o valor é`GUARDRAIL_INTERVENED` .
`guardrailSource`	O conteúdo que o guardrail avaliou. `INPUT`indica uma solicitação enviada ao modelo e `OUTPUT` indica uma resposta do modelo.
`contentPolicyFilters`	Uma lista dos filtros de política de conteúdo que o guardrail aplicou. Para esse tipo de descoberta, uma entrada tem um `type` de `PROMPT_ATTACK` e um `confidence` de`HIGH`. `action`É `BLOCKED` se a grade de proteção bloqueou o conteúdo ou `NONE` se a grade de proteção detectou o ataque imediato, mas foi configurada apenas para denunciá-lo.

Campo	Description
`sensitiveInformationFilters`	Filtros de informações confidenciais que o guardrail aplicou ao avaliar a invocação. Cada entrada identifica o tipo de informação confidencial detectada pela grade de proteção, como `AWS_SECRET_KEY` ou, e uma `type` que identifica se a grade `action` de proteção bloqueou o conteúdo`PASSWORD`, `BLOCKED` se a grade de proteção o mascarou ou `ANONYMIZED` `NONE` se a grade de proteção a detectou, mas foi configurada apenas para denunciá-la. A descoberta registra o tipo de informação detectada, nunca o conteúdo em si.

Essa descoberta corresponde à técnica MITRE ATLAS AML.T0051 - LLM Prompt Injection no site MITRE ATLAS.

Recomendações de correção:

Analise a solicitação que acionou a intervenção do guardrail e a identidade do IAM que enviou a solicitação. Se a atividade for inesperada para a identidade associada, as credenciais podem ter sido comprometidas. Para obter mais informações, consulte Correção de problemas potencialmente comprometidos AWS credenciais. Se a grade de proteção detectou, mas não bloqueou, o ataque imediato, considere definir a ação do filtro de conteúdo de ataque imediato como Bloquear em vez de Detectar, para que a grade de proteção bloqueie o conteúdo. Para obter mais informações, consulte Opções para lidar com conteúdo nocivo detectado pelo Amazon Bedrock Guardrails no Guia do usuário do Amazon Bedrock. Você também pode restringir o acesso às APIs de invocação do Amazon Bedrock para a identidade afetada.

Tipos de descoberta desabilitados

Uma descoberta é uma notificação que contém detalhes sobre um possível problema de segurança que o GuardDuty descobre. Para obter informações sobre mudanças importantes nos tipos de GuardDuty descoberta, incluindo tipos de descoberta recém-adicionados ou retirados, consulteHistórico de documentos da Amazon GuardDuty.

Os seguintes tipos de descoberta foram retirados e não são mais gerados pelo GuardDuty.

> **Important**
>
> Você não pode reativar tipos de GuardDuty descoberta desativados.

Tópicos

- PrivilegeEscalation:Kubernetes/PrivilegedContainer
- Persistence:Kubernetes/ContainerWithSensitiveMount
- Exfiltration:S3/ObjectRead.Unusual
- Impact:S3/PermissionsModification.Unusual
- Impact:S3/ObjectDelete.Unusual
- Discovery:S3/BucketEnumeration.Unusual
- Persistence:IAMUser/NetworkPermissions
- Persistence:IAMUser/ResourcePermissions
- Persistence:IAMUser/UserPermissions
- PrivilegeEscalation:IAMUser/AdministrativePermissions
- Recon:IAMUser/NetworkPermissions
- Recon:IAMUser/ResourcePermissions
- Recon:IAMUser/UserPermissions
- ResourceConsumption:IAMUser/ComputeResources
- Stealth:IAMUser/LoggingConfigurationModified
- UnauthorizedAccess:IAMUser/ConsoleLogin
- UnauthorizedAccess:EC2/TorIPCaller
- Backdoor:EC2/XORDDOS
- Behavior:IAMUser/InstanceLaunchUnusual
- CryptoCurrency:EC2/BitcoinTool.A
- UnauthorizedAccess:IAMUser/UnusualASNCaller

PrivilegeEscalation:Kubernetes/PrivilegedContainer

Um contêiner privilegiado com acesso de nível raiz foi lançado em seu cluster do Kubernetes.

Gravidade padrão: média

- Funcionalidade: logs de auditoria do EKS

Essa descoberta informa que um contêiner privilegiado foi lançado em seu cluster do Kubernetes usando uma imagem nunca antes usada para iniciar contêineres privilegiados em seu cluster. Um contêiner privilegiado tem acesso de nível raiz ao host. Os adversários podem lançar contêineres privilegiados como uma tática de escalonamento de privilégios para obter acesso e, em seguida, comprometer o host.

Recomendações de correção:

Se o lançamento desse contêiner for inesperado, as credenciais da identidade do usuário usadas para iniciar o contêiner poderão ser comprometidas. Revogue o acesso do usuário e reverta todas as alterações feitas por um adversário em seu cluster. Para obter mais informações, consulte Como corrigir as descobertas da Proteção do EKS.

Persistence:Kubernetes/ContainerWithSensitiveMount

Um contêiner foi lançado com um caminho de host externo sensível montado em seu interior.

Gravidade padrão: média

- Funcionalidade: logs de auditoria do EKS

Essa descoberta informa que um contêiner foi lançado com uma configuração que incluía um caminho de host confidencial com acesso de gravação na seção `volumeMounts`. Isso torna o caminho confidencial do host acessível e gravável de dentro do contêiner. Essa técnica é comumente usada por adversários para obter acesso ao sistema de arquivos do host.

Recomendações de correção:

Se o lançamento desse contêiner for inesperado, as credenciais da identidade do usuário usadas para iniciar o contêiner poderão ser comprometidas. Revogue o acesso do usuário e reverta todas as alterações feitas por um adversário em seu cluster. Para obter mais informações, consulte Como corrigir as descobertas da Proteção do EKS.

Se o lançamento desse contêiner for esperado, é recomendável usar uma regra de supressão que consiste em um critério de filtro com base no campo `resource.KubernetesDetails.KubernetesWorkloadDetails.containers.imagePrefix`. Nos critérios de filtro, o campo `imagePrefix` deve ser o mesmo que o `imagePrefix` especificado na descoberta. Para saber mais sobre a criação de regras de supressão, consulte Regras de supressão.

Exfiltration:S3/ObjectRead.Unusual

Uma entidade do IAM invocou uma API do S3 de forma suspeita.

Gravidade padrão: média*

> **Note**
>
> A gravidade padrão desta descoberta é Média. No entanto, se a API for invocada usando AWS credenciais temporárias criadas em uma instância, a severidade da descoberta será Alta.

- Fonte de dados: eventos CloudTrail de dados para S3

Essa descoberta informa que uma entidade do IAM em seu AWS ambiente está fazendo chamadas de API que envolvem um bucket do S3 e que diferem da linha de base estabelecida pela entidade. A chamada de API usada nessa atividade está associada ao estágio de exfiltração de um ataque, no qual um invasor está tentando coletar dados. Essa atividade é suspeita porque a forma como a entidade do IAM invocou a API era incomum. Por exemplo, essa entidade do IAM não tinha histórico anterior de invocação desse tipo de API, ou a API foi invocada de um local incomum.

Recomendações de correção:

Se essa atividade for inesperada para a entidade principal associada, isso pode indicar que as credenciais foram expostas ou que suas permissões do S3 não são restritivas o suficiente. Para obter mais informações, consulte Como corrigir um bucket do S3 possivelmente comprometido.

Impact:S3/PermissionsModification.Unusual

Uma entidade do IAM invocou uma API para modificar as permissões em um ou mais recursos do S3.

Gravidade padrão: média*

> **Note**
>
> A gravidade padrão desta descoberta é Média. No entanto, se a API for invocada usando AWS credenciais temporárias criadas em uma instância, a severidade da descoberta será Alta.

Essa descoberta informa que uma entidade do IAM está fazendo chamadas de API projetadas para modificar as permissões em um ou mais buckets ou objetos em seu ambiente da AWS . Essa ação pode ser executada por um invasor para permitir que as informações sejam compartilhadas fora da conta. Essa atividade é suspeita porque a forma como a entidade do IAM invocou a API era incomum. Por exemplo, essa entidade do IAM não tinha histórico anterior de invocação desse tipo de API, ou a API foi invocada de um local incomum.

Recomendações de correção:

Se essa atividade for inesperada para a entidade principal associada, isso pode indicar que as credenciais foram expostas ou que suas permissões do S3 não são restritivas o suficiente. Para obter mais informações, consulte Como corrigir um bucket do S3 possivelmente comprometido.

Impact:S3/ObjectDelete.Unusual

Uma entidade do IAM invocou uma API usada para excluir dados em um bucket do S3

Gravidade padrão: média*

> **Note**
>
> A gravidade padrão desta descoberta é Média. No entanto, se a API for invocada usando AWS credenciais temporárias criadas em uma instância, a severidade da descoberta será Alta.

Essa descoberta informa que uma entidade específica do IAM em seu AWS ambiente está fazendo chamadas de API projetadas para excluir dados no bucket do S3 listado, excluindo o próprio bucket. Essa atividade é suspeita porque a forma como a entidade do IAM invocou a API era incomum. Por exemplo, essa entidade do IAM não tinha histórico anterior de invocação desse tipo de API, ou a API foi invocada de um local incomum.

Recomendações de correção:

Se essa atividade for inesperada para a entidade principal associada, isso pode indicar que as credenciais foram expostas ou que suas permissões do S3 não são restritivas o suficiente. Para obter mais informações, consulte Como corrigir um bucket do S3 possivelmente comprometido.

Discovery:S3/BucketEnumeration.Unusual

Uma entidade do IAM invocou uma API do S3 usada para descobrir buckets do S3 na sua rede.

Gravidade padrão: média*

> **Note**
>
> A gravidade padrão desta descoberta é Média. No entanto, se a API for invocada usando AWS credenciais temporárias criadas em uma instância, a severidade da descoberta será Alta.

Essa descoberta informa que uma entidade do IAM invocou uma API do S3 para descobrir buckets do S3 em seu ambiente, como `ListBuckets`. Esse tipo de atividade está associado ao estágio de descoberta de um ataque, no qual um invasor coleta informações para determinar se seu AWS ambiente é suscetível a um ataque mais amplo. Essa atividade é suspeita porque a forma como a entidade do IAM invocou a API era incomum. Por exemplo, essa entidade do IAM não tinha histórico anterior de invocação desse tipo de API, ou a API foi invocada de um local incomum.

Recomendações de correção:

Se essa atividade for inesperada para a entidade principal associada, isso pode indicar que as credenciais foram expostas ou que suas permissões do S3 não são restritivas o suficiente. Para obter mais informações, consulte Como corrigir um bucket do S3 possivelmente comprometido.

Persistence:IAMUser/NetworkPermissions

Uma entidade do IAM invocou uma API comumente usada para alterar as permissões de acesso à rede para grupos de segurança, rotas e ACLs em seu AWS conta.

Gravidade padrão: média*

> **Note**
>
> A gravidade padrão desta descoberta é Média. No entanto, se a API for invocada usando AWS credenciais temporárias criadas em uma instância, a severidade da descoberta será Alta.

Essa descoberta indica que um diretor específico (Usuário raiz da conta da AWS, função do IAM ou usuário) em seu AWS ambiente está exibindo um comportamento diferente da linha de base estabelecida. Essa entidade principal não tem histórico prévio de invocação dessa API.

Essa descoberta é acionada quando as configurações de rede são alteradas em circunstâncias suspeitas, como quando uma entidade principal invoca a API `CreateSecurityGroup` sem nenhum histórico anterior de fazer isso. Os invasores geralmente tentam alterar os grupos de segurança para permitir determinados tráfegos de entrada em várias portas para melhorar sua capacidade de acessar uma instância do EC2.

Recomendações de correção:

Se essa atividade for inesperada, suas credenciais podem estar comprometidas. Para obter mais informações, consulte Correção de problemas potencialmente comprometidos AWS credenciais.

Persistence:IAMUser/ResourcePermissions

Um diretor invocou uma API comumente usada para alterar as políticas de acesso de segurança de vários recursos em seu Conta da AWS.

Gravidade padrão: média*

> **Note**
>
> A gravidade padrão desta descoberta é Média. No entanto, se a API for invocada usando AWS credenciais temporárias criadas em uma instância, a severidade da descoberta será Alta.

Essa descoberta indica que um diretor específico (Usuário raiz da conta da AWS, função do IAM ou usuário) em seu AWS ambiente está exibindo um comportamento diferente da linha de base estabelecida. Essa entidade principal não tem histórico prévio de invocação dessa API.

Essa descoberta é acionada quando uma alteração é detectada nas políticas ou permissões associadas aos AWS recursos, como quando um diretor em seu AWS ambiente invoca a `PutBucketPolicy` API sem nenhum histórico anterior de fazer isso. Alguns serviços, como o Amazon S3, oferecem suporte a permissões anexadas a recursos que garantem um ou mais acessos de principais ao recurso. Com credenciais roubadas, os invasores podem alterar as políticas anexadas a um recurso, para conseguir acesso a esse recurso.

Recomendações de correção:

Se essa atividade for inesperada, suas credenciais podem estar comprometidas. Para obter mais informações, consulte Correção de problemas potencialmente comprometidos AWS credenciais.

Persistence:IAMUser/UserPermissions

Um principal invocou uma API comumente usada para adicionar, modificar ou excluir usuários, grupos ou políticas do IAM em seu AWS conta.

Gravidade padrão: média*

> **Note**
>
> A gravidade padrão desta descoberta é Média. No entanto, se a API for invocada usando AWS credenciais temporárias criadas em uma instância, a severidade da descoberta será Alta.

Essa descoberta indica que um diretor específico (Usuário raiz da conta da AWS, função do IAM ou usuário) em seu AWS ambiente está exibindo um comportamento diferente da linha de base estabelecida. Essa entidade principal não tem histórico prévio de invocação dessa API.

Essa descoberta é acionada por alterações suspeitas nas permissões relacionadas ao usuário em seu AWS ambiente, como quando um diretor em seu AWS ambiente invoca a `AttachUserPolicy` API sem nenhum histórico anterior de fazer isso. Os invasores podem usar credenciais roubadas para criar novos usuários, adicionar políticas de acesso aos usuários existentes ou criar chaves de acesso para maximizar o acesso a uma conta, mesmo que o ponto de acesso original esteja fechado. Por exemplo, o proprietário da conta pode perceber que um determinado usuário ou senha do IAM foi roubado e excluí-lo da conta. No entanto, eles não podem excluir outros usuários que foram criados por um administrador principal criado de forma fraudulenta, deixando sua AWS conta acessível ao invasor.

Recomendações de correção:

Se essa atividade for inesperada, suas credenciais podem estar comprometidas. Para obter mais informações, consulte Correção de problemas potencialmente comprometidos AWS credenciais.

PrivilegeEscalation:IAMUser/AdministrativePermissions

Um principal tentou atribuir uma política altamente permissiva a si próprio.

Gravidade padrão: baixa*

> **Note**
>
> Essa descoberta da gravidade é baixa se a tentativa de escalonamento de privilégios não foi bem-sucedida e média se a tentativa de escalonamento foi bem-sucedida.

Essa descoberta indica que uma entidade específica do IAM em seu AWS ambiente está exibindo um comportamento que pode ser indicativo de um ataque de escalonamento de privilégios. Essa descoberta é acionada quando um usuário ou perfil do IAM tenta atribuir uma política altamente permissiva a si próprio. Se o usuário ou o perfil em questão não deve ter privilégios administrativos, isso indica que as credenciais do usuário podem estar comprometidas ou que as permissões do perfil podem estar configuradas inadequadamente.

Os invasores usarão credenciais roubadas para criar novos usuários, adicionar políticas de acesso aos usuários existentes ou criar chaves de acesso para maximizar o acesso a uma conta, mesmo

que o ponto de acesso original esteja fechado. Por exemplo, o proprietário da conta pode perceber que a credencial de login de um determinado usuário do IAM foi roubada e excluí-lo da conta, mas pode não excluir outros usuários que foram criados por um diretor administrativo criado de forma fraudulenta, deixando sua conta da AWS ainda acessível ao invasor.

Recomendações de correção:

Se essa atividade for inesperada, suas credenciais podem estar comprometidas. Para obter mais informações, consulte Correção de problemas potencialmente comprometidos AWS credenciais.

Recon:IAMUser/NetworkPermissions

Um diretor invocou uma API comumente usada para alterar as permissões de acesso à rede para grupos de segurança, rotas e ACLs em seu AWS conta.

Gravidade padrão: média*

> **Note**
>
> A gravidade padrão desta descoberta é Média. No entanto, se a API for invocada usando AWS credenciais temporárias criadas em uma instância, a severidade da descoberta será Alta.

Essa descoberta indica que um diretor específico (Usuário raiz da conta da AWS, função do IAM ou usuário) em seu AWS ambiente está exibindo um comportamento diferente da linha de base estabelecida. Essa entidade principal não tem histórico prévio de invocação dessa API.

Essa descoberta é acionada quando as permissões de acesso de recurso em sua conta da AWS são examinadas quanto a circunstâncias duvidosas. Por exemplo, se uma entidade principal sem histórico de fazer isso invocou a API `DescribeInstances`. Um invasor pode usar credenciais roubadas para realizar esse tipo de reconhecimento de seus AWS recursos a fim de encontrar credenciais mais valiosas ou determinar as capacidades das credenciais que ele já possui.

Recomendações de correção:

Se essa atividade for inesperada, suas credenciais podem estar comprometidas. Para obter mais informações, consulte Correção de problemas potencialmente comprometidos AWS credenciais.

Recon:IAMUser/ResourcePermissions

Um diretor invocou uma API comumente usada para alterar as políticas de acesso de segurança de vários recursos em seu AWS conta.

Gravidade padrão: média*

> **Note**
>
> A gravidade padrão desta descoberta é Média. No entanto, se a API for invocada usando AWS credenciais temporárias criadas em uma instância, a severidade da descoberta será Alta.

Essa descoberta indica que um diretor específico (Usuário raiz da conta da AWS, função do IAM ou usuário) em seu AWS ambiente está exibindo um comportamento diferente da linha de base estabelecida. Essa entidade principal não tem histórico prévio de invocação dessa API.

Essa descoberta é acionada quando as permissões de acesso de recurso em sua conta da AWS são examinadas quanto a circunstâncias duvidosas. Por exemplo, se uma entidade principal sem histórico de fazer isso invocou a API `DescribeInstances`. Um invasor pode usar credenciais roubadas para realizar esse tipo de reconhecimento de seus AWS recursos a fim de encontrar credenciais mais valiosas ou determinar as capacidades das credenciais que ele já possui.

Recomendações de correção:

Se essa atividade for inesperada, suas credenciais podem estar comprometidas. Para obter mais informações, consulte Correção de problemas potencialmente comprometidos AWS credenciais.

Recon:IAMUser/UserPermissions

Um principal invocou uma API comumente usada para adicionar, modificar ou excluir usuários, grupos ou políticas do IAM em seu AWS conta.

Gravidade padrão: média*

> **Note**
>
> A gravidade padrão desta descoberta é Média. No entanto, se a API for invocada usando AWS credenciais temporárias criadas em uma instância, a severidade da descoberta será Alta.

Essa descoberta é acionada quando as permissões do usuário em seu AWS ambiente são investigadas sob circunstâncias suspeitas. Por exemplo, se uma entidade principal (Usuário raiz da conta da AWS, perfil do IAM ou usuário do IAM) invocou a API `ListInstanceProfilesForRole` sem histórico de fazer isso. Um invasor pode usar credenciais roubadas para realizar esse tipo de reconhecimento de seus AWS recursos a fim de encontrar credenciais mais valiosas ou determinar as capacidades das credenciais que ele já possui.

Essa descoberta indica que um diretor específico em seu AWS ambiente está exibindo um comportamento diferente da linha de base estabelecida. Essa entidade principal não tem histórico de invocar essa API dessa maneira.

Recomendações de correção:

Se essa atividade for inesperada, suas credenciais podem estar comprometidas. Para obter mais informações, consulte Correção de problemas potencialmente comprometidos AWS credenciais.

ResourceConsumption:IAMUser/ComputeResources

Um principal invocou uma API comumente usada para executar recursos de computação, como instâncias do EC2.

Gravidade padrão: média*

> **Note**
>
> A gravidade padrão desta descoberta é Média. No entanto, se a API for invocada usando AWS credenciais temporárias criadas em uma instância, a severidade da descoberta será Alta.

Essa descoberta é acionada quando as instâncias do EC2 na conta listada em seu ambiente da AWS são iniciadas em circunstâncias suspeitas. Essa descoberta indica que um principal específico

em seu AWS ambiente está exibindo um comportamento diferente da linha de base estabelecida; por exemplo, se um principal (Usuário raiz da conta da AWS, função do IAM ou usuário do IAM) invocou a `RunInstances` API sem histórico anterior de fazer isso. Isso pode ser uma indicação de que um invasor está usando credenciais roubadas para roubar tempo de computação (possivelmente para mineração de criptomoeda ou quebra de senhas). Também pode ser uma indicação de que um invasor está usando uma instância do EC2 em seu AWS ambiente e suas credenciais para manter o acesso à sua conta.

Recomendações de correção:

Se essa atividade for inesperada, suas credenciais podem estar comprometidas. Para obter mais informações, consulte Correção de problemas potencialmente comprometidos AWS credenciais.

Stealth:IAMUser/LoggingConfigurationModified

Um diretor invocou uma API comumente usada para interromper o CloudTrail registro, excluir registros existentes e, de outra forma, eliminar traços de atividade em seu AWS conta.

Gravidade padrão: média*

> **Note**
>
> A gravidade padrão desta descoberta é Média. No entanto, se a API for invocada usando AWS credenciais temporárias criadas em uma instância, a severidade da descoberta será Alta.

Essa descoberta é acionada quando a configuração de registro na conta da AWS listada em seu ambiente é modificada em circunstâncias suspeitas. Essa descoberta informa que um principal específico em seu AWS ambiente está exibindo um comportamento diferente da linha de base estabelecida; por exemplo, se um principal (Usuário raiz da conta da AWS, função do IAM ou usuário do IAM) invocou a `StopLogging` API sem histórico anterior de fazer isso. Isso pode ser uma indicação de que um invasor está tentando encobrir os próprios rastros eliminando qualquer traço de atividade dele.

Recomendações de correção:

Se essa atividade for inesperada, suas credenciais podem estar comprometidas. Para obter mais informações, consulte Correção de problemas potencialmente comprometidos AWS credenciais.

UnauthorizedAccess:IAMUser/ConsoleLogin

Um login incomum no console feito por um diretor em seu AWS conta foi observada.

Gravidade padrão: média*

> **Note**
>
> A gravidade padrão desta descoberta é Média. No entanto, se a API for invocada usando AWS credenciais temporárias criadas em uma instância, a severidade da descoberta será Alta.

Essa descoberta é acionada quando um login no console é detectado em circunstâncias duvidosas. Por exemplo, se um principal sem histórico anterior de fazer isso invocou a ConsoleLogin API de um cliente nunca antes usado ou de um local incomum. Isso pode ser uma indicação de que credenciais roubadas estão sendo usadas para obter acesso à sua AWS conta ou de um usuário válido acessando a conta de maneira inválida ou menos segura (por exemplo, não por meio de uma VPN aprovada).

Essa descoberta informa que um diretor específico em seu AWS ambiente está exibindo um comportamento diferente da linha de base estabelecida. Essa entidade principal não tem histórico de atividades de login usando essa aplicação cliente a partir desse local específico.

Recomendações de correção:

Se essa atividade for inesperada, suas credenciais podem estar comprometidas. Para obter mais informações, consulte Correção de problemas potencialmente comprometidos AWS credenciais.

UnauthorizedAccess:EC2/TorIPCaller

A instância do EC2 está recebendo conexões de entrada de um nó de saída Tor.

Gravidade padrão: média

Essa descoberta informa que uma instância do EC2 em seu AWS ambiente está recebendo conexões de entrada de um nó de saída do Tor. Tor é um software para permitir a comunicação

anônima. Ele criptografa e aleatoriamente envia comunicações por meio de relés entre uma série de nós de rede. O último nó do Tor é chamado de nó de saída. Essa descoberta pode indicar acesso não autorizado aos seus AWS recursos com a intenção de ocultar a verdadeira identidade do atacante.

Recomendações de correção:

Se essa atividade for inesperada, sua instância pode estar comprometida. Para obter mais informações, consulte Como corrigir uma instância do Amazon EC2 potencialmente comprometida.

Backdoor:EC2/XORDDOS

Uma instância do EC2 está tentando se comunicar com um endereço IP associado ao malware XorDDos.

Gravidade padrão: alta

Essa descoberta informa que uma instância do EC2 em seu AWS ambiente está tentando se comunicar com um endereço IP associado ao malware XOR DDoS. Essa instância do EC2 pode estar comprometida. O XOR DDoS é um malware de Trojan que sequestra sistemas Linux. Para ter acesso ao sistema, ele lança um ataque de força bruta e descobre a senha dos serviços Secure Shell (SSH) no Linux. Quando as credenciais do SSH são adquiridas e o login é realizado com sucesso, ele usa privilégios de root para executar um script que faz download e instala o XOR DDoS. Em seguida, esse malware é usado como parte de um botnet para iniciar ataques de negação de serviço distribuída (DDoS) contra outros alvos.

Recomendações de correção:

Se essa atividade for inesperada, sua instância pode estar comprometida. Para obter mais informações, consulte Como corrigir uma instância do Amazon EC2 potencialmente comprometida.

Behavior:IAMUser/InstanceLaunchUnusual

Um usuário do IAM lançou uma instância do EC2 de um tipo incomum.

Gravidade padrão: alta

Essa descoberta informa que um usuário específico em seu AWS ambiente está exibindo um comportamento diferente da linha de base estabelecida. Esse usuário não possui histórico prévio de iniciar uma instância do EC2 desse tipo. Suas credenciais podem estar comprometidas.

Recomendações de correção:

Se essa atividade for inesperada, suas credenciais podem estar comprometidas. Para obter mais informações, consulte Correção de problemas potencialmente comprometidos AWS credenciais.

CryptoCurrency:EC2/BitcoinTool.A

A instância do EC2 está se comunicando com os pools de mineração do Bitcoin.

Gravidade padrão: alta

Essa descoberta informa que uma instância do EC2 em seu AWS ambiente está se comunicando com os pools de mineração de Bitcoin. No campo da mineração de criptomoeda, um grupo de mineração refere-se ao agrupamento de recursos por mineiros que compartilham o poder de processamento deles em uma rede para dividir a recompensa de acordo com a quantidade de trabalho que ofereceram para resolver um bloco. A menos que você use essa instância do EC2 para a mineração de Bitcoin, sua instância do EC2 pode estar comprometida.

Recomendações de correção:

Se essa atividade for inesperada, sua instância pode estar comprometida. Para obter mais informações, consulte Como corrigir uma instância do Amazon EC2 potencialmente comprometida.

UnauthorizedAccess:IAMUser/UnusualASNCaller

Uma API foi invocada a partir de um endereço IP de uma rede incomum.

Gravidade padrão: alta

Essa descoberta informa que determinada atividade foi invocada a partir de um endereço IP de uma rede incomum. Essa rede nunca foi observada em todo o histórico de uso da AWS do usuário descrito. Essa atividade pode incluir um login no console, uma tentativa de iniciar uma instância do EC2, a criação de um novo usuário do IAM ou a modificação de seus privilégios da AWS , etc. Isso pode indicar acesso não autorizado aos seus AWS recursos.

Recomendações de correção:

Se essa atividade for inesperada, suas credenciais podem estar comprometidas. Para obter mais informações, consulte Correção de problemas potencialmente comprometidos AWS credenciais.

GuardDuty encontrando tipos por meio de recursos potencialmente afetados

As páginas a seguir são categorizadas pelo tipo de recurso potencialmente afetado associado a uma GuardDuty descoberta:

- Tipos de descoberta do EC2
- Tipos de descobertas do IAM
- Tipos de descoberta de sequência de ataque
- Tipos de localização de regras de detecção personalizadas
- Tipos de descoberta da Proteção do S3
- Tipos de descoberta da Proteção do EKS
- Tipos de descoberta do Monitoramento de runtime
- Tipos de descoberta da Proteção contra malware para EC2
- Tipo de descoberta da Proteção contra malware para S3
- Proteção contra malware para tipos de descoberta de Backup
- Tipos de descoberta da Proteção do RDS
- Tipos de descoberta da Proteção do Lambda
- Tipos de descoberta de proteção de IA

GuardDuty tipos de descoberta ativa

A tabela a seguir mostra todos os tipos de descobertas ativas, agrupados por sua origem: primeiro os tipos de descoberta da detecção básica de ameaças (classificados por fonte de dados), depois os tipos de descoberta da sequência de Detecção de Ameaças Avançada ataque e, em seguida, os tipos de descoberta de cada plano de proteção (em ordem alfabética por plano). Na tabela a seguir, algumas das descobertas têm os valores da coluna Gravidade da descoberta marcados com um asterisco (*) ou um sinal de adição (+):

*Esses tipos de descoberta têm gravidade variável. Uma descoberta de um tipo específico pode ter uma gravidade diferente dependendo do contexto específico da descoberta. Para obter mais informações sobre um tipo de descoberta, veja sua descrição detalhada.

[+]As descobertas do EC2 que usam logs de fluxo da VPC como fonte de dados não oferecem suporte ao tráfego IPv6.

Tipo de descoberta	Tipo de atributo	Dados fundamentais source/Feature	Gravidade da descoberta
CredentialAccess:IAMUser/AnomalousBehavior	IAM	CloudTrail eventos de gerenciamento	Médio
DefenseEvasion:IAMUser/AnomalousBehavior	IAM	CloudTrail eventos de gerenciamento	Médio
DefenseEvasion:IAMUser/BedrockLoggingDisabled	IAM	CloudTrail eventos de gerenciamento	Médio
Discovery:IAMUser/AnomalousBehavior	IAM	CloudTrail eventos de gerenciamento	Baixo
Exfiltration:IAMUser/AnomalousBehavior	IAM	CloudTrail eventos de gerenciamento	Alto
Impact:IAMUser/AnomalousBehavior	IAM	CloudTrail eventos de gerenciamento	Alto
InitialAccess:IAMUser/AnomalousBehavior	IAM	CloudTrail eventos de gerenciamento	Médio
PenTest:IAMUser/KaliLinux	IAM	CloudTrail eventos de gerenciamento	Médio
PenTest:IAMUser/ParrotLinux	IAM	CloudTrail eventos de gerenciamento	Médio
PenTest:IAMUser/PentooLinux	IAM	CloudTrail eventos de gerenciamento	Médio

Tipo de descoberta	Tipo de atributo	Dados fundamentais source/Feature	Gravidade da descoberta
Persistence:IAMUser/AnomalousBehavior	IAM	CloudTrail eventos de gerenciamento	Médio
Stealth:IAMUser/PasswordPolicyChange	IAM	CloudTrail eventos de gerenciamento	Baixo *
UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.InsideAWS	IAM	CloudTrail eventos de gerenciamento	Alto *
Policy:S3/AccountBlockPublicAccessDisabled	Amazon S3	CloudTrail eventos de gerenciamento	Baixo
Policy:S3/BucketAnonymousAccessGranted	Amazon S3	CloudTrail eventos de gerenciamento	Alto
Policy:S3/BucketBlockPublicAccessDisabled	Amazon S3	CloudTrail eventos de gerenciamento	Baixo
Policy:S3/BucketPublicAccessGranted	Amazon S3	CloudTrail eventos de gerenciamento	Alto
PrivilegeEscalation:IAMUser/AnomalousBehavior	IAM	CloudTrail eventos de gerenciamento	Médio
Recon:IAMUser/MaliciousIPCaller	IAM	CloudTrail eventos de gerenciamento	Médio
Recon:IAMUser/MaliciousIPCaller.Custom	IAM	CloudTrail eventos de gerenciamento	Médio

Tipo de descoberta	Tipo de atributo	Dados fundamentais source/Feature	Gravidade da descoberta
Recon:IAMUser/TorIPCaller	IAM	CloudTrail eventos de gerenciamento	Médio
Stealth:IAMUser/CloudTrailLoggingDisabled	IAM	CloudTrail eventos de gerenciamento	Baixo
Stealth:S3/ServerAccessLoggingDisabled	Amazon S3	CloudTrail eventos de gerenciamento	Baixo
UnauthorizedAccess:IAMUser/ConsoleLoginSuccess.B	IAM	CloudTrail eventos de gerenciamento	Médio
UnauthorizedAccess:IAMUser/MaliciousIPCaller	IAM	CloudTrail eventos de gerenciamento	Médio
UnauthorizedAccess:IAMUser/MaliciousIPCaller.Custom	IAM	CloudTrail eventos de gerenciamento	Médio
UnauthorizedAccess:IAMUser/TorIPCaller	IAM	CloudTrail eventos de gerenciamento	Médio
CredentialAccess:IAMUser/CompromisedCredentials	IAM	CloudTrail eventos de gerenciamento ou eventos CloudTrail de dados para o S3	Alto
Policy:IAMUser/RootCredentialUsage	IAM	CloudTrail eventos de gerenciamento ou eventos CloudTrail de dados para o S3	Baixo

Tipo de descoberta	Tipo de atributo	Dados fundamentais source/Feature	Gravidade da descoberta
Policy:IAMUser/ShortTermRootCredentialUsage	IAM	CloudTrail eventos de gerenciamento ou eventos CloudTrail de dados para o S3	Baixo
UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS	IAM	CloudTrail eventos de gerenciamento ou eventos CloudTrail de dados para o S3	Alto
UnauthorizedAccess:IAMUser/ResourceCredentialExfiltration.InsideAWS	IAM	CloudTrail eventos de gerenciamento ou eventos CloudTrail de dados para o S3	Alto
UnauthorizedAccess:IAMUser/ResourceCredentialExfiltration.OutsideAWS	IAM	CloudTrail eventos de gerenciamento ou eventos CloudTrail de dados para o S3	Alto
Impact:EC2/MaliciousDomainRequest.Custom	Amazon EC2	Logs de DNS	Médio
Backdoor:EC2/C&CActivity.B!DNS	Amazon EC2	Logs de DNS	Alto
CryptoCurrency:EC2/BitcoinTool.B!DNS	Amazon EC2	Logs de DNS	Alto
Impact:EC2/AbusedDomainRequest.Reputation	Amazon EC2	Logs de DNS	Médio

Tipo de descoberta	Tipo de atributo	Dados fundamentais source/Feature	Gravidade da descoberta
Impact:EC2/BitcoinDomainRequest.Reputation	Amazon EC2	Logs de DNS	Alto
Impact:EC2/MaliciousDomainRequest.Reputation	Amazon EC2	Logs de DNS	Alto
Impact:EC2/SuspiciousDomainRequest.Reputation	Amazon EC2	Logs de DNS	Baixo
Trojan:EC2/BlackholeTraffic!DNS	Amazon EC2	Logs de DNS	Médio
Trojan:EC2/DGADomainRequest.B	Amazon EC2	Logs de DNS	Alto
Trojan:EC2/DGADomainRequest.C!DNS	Amazon EC2	Logs de DNS	Alto
Trojan:EC2/DNSDataExfiltration	Amazon EC2	Logs de DNS	Alto
Trojan:EC2/DriveBySourceTraffic!DNS	Amazon EC2	Logs de DNS	Alto
Trojan:EC2/DropPoint!DNS	Amazon EC2	Logs de DNS	Médio
Trojan:EC2/PhishingDomainRequest!DNS	Amazon EC2	Logs de DNS	Alto

Tipo de descoberta	Tipo de atributo	Dados fundamentais source/Feature	Gravidade da descoberta
UnauthorizedAccess:EC2/MetadataDNSRebind	Amazon EC2	Logs de DNS	Alto
Backdoor:EC2/C&CActivity.B	Amazon EC2	Registros de fluxo de VPC ±	Alto
Backdoor:EC2/DenialOfService.Dns	Amazon EC2	Registros de fluxo de VPC ±	Alto
Backdoor:EC2/DenialOfService.Tcp	Amazon EC2	Registros de fluxo de VPC ±	Alto
Backdoor:EC2/DenialOfService.Udp	Amazon EC2	Registros de fluxo de VPC ±	Alto
Backdoor:EC2/DenialOfService.UdpOnTcpPorts	Amazon EC2	Registros de fluxo de VPC ±	Alto
Backdoor:EC2/DenialOfService.UnusualProtocol	Amazon EC2	Registros de fluxo de VPC ±	Alto
Backdoor:EC2/Spambot	Amazon EC2	Registros de fluxo de VPC ±	Médio
Behavior:EC2/NetworkPortUnusual	Amazon EC2	Registros de fluxo de VPC ±	Médio
Behavior:EC2/TrafficVolumeUnusual	Amazon EC2	Registros de fluxo de VPC ±	Médio

Tipo de descoberta	Tipo de atributo	Dados fundamentais source/Feature	Gravidade da descoberta
CryptoCurrency:EC2/BitcoinTool.B	Amazon EC2	Registros de fluxo de VPC +	Alto
DefenseEvasion:EC2/UnusualDNSResolver	Amazon EC2	Registros de fluxo de VPC +	Médio
DefenseEvasion:EC2/UnusualDoHActivity	Amazon EC2	Registros de fluxo de VPC +	Médio
DefenseEvasion:EC2/UnusualDoTActivity	Amazon EC2	Registros de fluxo de VPC +	Médio
Impact:EC2/PortSweep	Amazon EC2	Registros de fluxo de VPC +	Alto
Impact:EC2/WinRMBruteForce	Amazon EC2	Registros de fluxo de VPC +	Baixo *
Recon:EC2/PortProbeEMRUnprotectedPort	Amazon EC2	Registros de fluxo de VPC +	Alto
Recon:EC2/PortProbeUnprotectedPort	Amazon EC2	Registros de fluxo de VPC +	Baixo *
Recon:EC2/Portscan	Amazon EC2	Registros de fluxo de VPC +	Médio
Trojan:EC2/BlackholeTraffic	Amazon EC2	Registros de fluxo de VPC +	Médio
Trojan:EC2/DropPoint	Amazon EC2	Registros de fluxo de VPC +	Médio

Tipo de descoberta	Tipo de atributo	Dados fundamentais source/Feature	Gravidade da descoberta
UnauthorizedAccess:EC2/MaliciousIPCaller.Custom	Amazon EC2	Registros de fluxo de VPC [+]	Médio
UnauthorizedAccess:EC2/RDPBruteForce	Amazon EC2	Registros de fluxo de VPC [+]	Baixo [*]
UnauthorizedAccess:EC2/SSHBruteForce	Amazon EC2	Registros de fluxo de VPC [+]	Baixo [*]
UnauthorizedAccess:EC2/TorClient	Amazon EC2	Registros de fluxo de VPC [+]	Alto
UnauthorizedAccess:EC2/TorRelay	Amazon EC2	Registros de fluxo de VPC [+]	Alto

Tipo de descoberta	Tipo de atributo	Dados fundamentais source/Feature	Gravidade da descoberta
AttackSequence:EKS/CompromisedCluster	Recursos envolvidos na sequência de ataque	• Eventos de log de auditoria do EKS • Monitoramento de Runtime para Amazon EKS • Detecção de malware no Amazon EKS para Amazon EC2 • AWS CloudTrail eventos de dados para S3 • AWS CloudTrail eventos de gerenciamento • Logs de fluxo da VPC • Logs de consultas de DNS do Route53 Resolver	Crítico
AttackSequence:IAM/CompromisedCredentials	Recursos envolvidos na sequência de ataque	CloudTrail eventos de gerenciamento	Crítico
AttackSequence:S3/CompromisedData	Recursos envolvidos na sequência de ataque	CloudTrail eventos de gerenciamento e eventos CloudTrail de dados para S3	Crítico

Tipo de descoberta	Tipo de atributo	Dados fundamentais source/Feature	Gravidade da descoberta
AttackSequence:ECS/CompromisedCluster	Recursos envolvidos na sequência de ataque	• AWS Detecções do Amazon ECS Runtime (Fargate) • AWS Detecções de tempo de execução do Amazon ECS (instâncias do Amazon EC2) • AWS Detecções de malware	Crítico
AttackSequence:EC2/CompromisedInstanceGroup	Recursos envolvidos na sequência de ataque	• AWS Detecções de tempo de execução do Amazon EC2 • AWS Detecções de malware • Logs de fluxo da VPC • Logs de consultas de DNS do Route53 Resolver	Crítico
Impact:IAMUser/AnomalousModelInvocation	IAM	Proteção da IA	Baixo
Impact:IAMUser/CostHarvesting	IAM	Proteção da IA	Baixo
Impact:IAMUser/PromptInjection.Direct	IAM	Proteção da IA	Baixo

Tipo de descoberta	Tipo de atributo	Dados fundamentais source/Feature	Gravidade da descoberta
CredentialAccess:Kubernetes/AnomalousBehavior.SecretsAccessed	Kubernetes	Logs de auditoria do EKS	Médio
CredentialAccess:Kubernetes/MaliciousIPCaller	Kubernetes	Logs de auditoria do EKS	Alto
CredentialAccess:Kubernetes/MaliciousIPCaller.Custom	Kubernetes	Logs de auditoria do EKS	Alto
CredentialAccess:Kubernetes/SuccessfulAnonymousAccess	Kubernetes	Logs de auditoria do EKS	Alto
CredentialAccess:Kubernetes/TorIPCaller	Kubernetes	Logs de auditoria do EKS	Alto
DefenseEvasion:Kubernetes/MaliciousIPCaller	Kubernetes	Logs de auditoria do EKS	Alto
DefenseEvasion:Kubernetes/MaliciousIPCaller.Custom	Kubernetes	Logs de auditoria do EKS	Alto
DefenseEvasion:Kubernetes/SuccessfulAnonymousAccess	Kubernetes	Logs de auditoria do EKS	Alto
DefenseEvasion:Kubernetes/TorIPCaller	Kubernetes	Logs de auditoria do EKS	Alto

Tipo de descoberta	Tipo de atributo	Dados fundamentais source/Feature	Gravidade da descoberta
Discovery:Kubernetes/AnomalousBehavior.PermissionChecked	Kubernetes	Logs de auditoria do EKS	Baixo
Discovery:Kubernetes/MaliciousIPCaller	Kubernetes	Logs de auditoria do EKS	Médio
Discovery:Kubernetes/MaliciousIPCaller.Custom	Kubernetes	Logs de auditoria do EKS	Médio
Discovery:Kubernetes/SuccessfulAnonymousAccess	Kubernetes	Logs de auditoria do EKS	Médio
Discovery:Kubernetes/TorIPCaller	Kubernetes	Logs de auditoria do EKS	Médio
Execution:Kubernetes/ExecInKubeSystemPod	Kubernetes	Logs de auditoria do EKS	Médio
Execution:Kubernetes/AnomalousBehavior.ExecInPod	Kubernetes	Logs de auditoria do EKS	Médio
Execution:Kubernetes/AnomalousBehavior.WorkloadDeployed	Kubernetes	Logs de auditoria do EKS	Baixo
Impact:Kubernetes/MaliciousIPCaller	Kubernetes	Logs de auditoria do EKS	Alto

Tipo de descoberta	Tipo de atributo	Dados fundamentais source/Feature	Gravidade da descoberta
Impact:Kubernetes/MaliciousIPCaller.Custom	Kubernetes	Logs de auditoria do EKS	Alto
Impact:Kubernetes/SuccessfulAnonymousAccess	Kubernetes	Logs de auditoria do EKS	Alto
Impact:Kubernetes/TorIPCaller	Kubernetes	Logs de auditoria do EKS	Alto
Persistence:Kubernetes/MaliciousIPCaller	Kubernetes	Logs de auditoria do EKS	Médio
Persistence:Kubernetes/MaliciousIPCaller.Custom	Kubernetes	Logs de auditoria do EKS	Médio
Persistence:Kubernetes/SuccessfulAnonymousAccess	Kubernetes	Logs de auditoria do EKS	Alto
Persistence:Kubernetes/TorIPCaller	Kubernetes	Logs de auditoria do EKS	Médio
Policy:Kubernetes/AdminAccessToDefaultServiceAccount	Kubernetes	Logs de auditoria do EKS	Alto
Policy:Kubernetes/AnonymousAccessGranted	Kubernetes	Logs de auditoria do EKS	Alto
Policy:Kubernetes/KubeflowDashboardExposed	Kubernetes	Logs de auditoria do EKS	Médio

Tipo de descoberta	Tipo de atributo	Dados fundamentais source/Feature	Gravidade da descoberta
Policy:Kubernetes/ExposedDashboard	Kubernetes	Logs de auditoria do EKS	Médio
PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleBindingCreated	Kubernetes	Logs de auditoria do EKS	Médio *
PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleCreated	Kubernetes	Logs de auditoria do EKS	Baixo
Persistence:Kubernetes/AnomalousBehavior.WorkloadDeployed!ContainerWithSensitiveMount	Kubernetes	Logs de auditoria do EKS	Alto
PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!PrivilegedContainer	Kubernetes	Logs de auditoria do EKS	Alto
Backdoor:Lambda/C&CActivity.B	Lambda	Monitoramento de atividades da rede Lambda	Alto
CryptoCurrency:Lambda/BitcoinTool.B	Lambda	Monitoramento de atividades da rede Lambda	Alto

Tipo de descoberta	Tipo de atributo	Dados fundamentais source/Feature	Gravidade da descoberta
Trojan:Lambda/BlackholeTraffic	Lambda	Monitoramento de atividades da rede Lambda	Médio
Trojan:Lambda/DropPoint	Lambda	Monitoramento de atividades da rede Lambda	Médio
UnauthorizedAccess:Lambda/MaliciousIPCaller.Custom	Lambda	Monitoramento de atividades da rede Lambda	Médio
UnauthorizedAccess:Lambda/TorClient	Lambda	Monitoramento de atividades da rede Lambda	Alto
UnauthorizedAccess:Lambda/TorRelay	Lambda	Monitoramento de atividades da rede Lambda	Alto
Execution:Container/MaliciousFile	Contêiner	Proteção contra malware EBS	Varia de acordo com a ameaça detectada
Execution:Container/SuspiciousFile	Contêiner	Proteção contra malware EBS	Varia de acordo com a ameaça detectada
Execution:EC2/MaliciousFile	Amazon EC2	Proteção contra malware EBS	Varia de acordo com a ameaça detectada
Execution:EC2/SuspiciousFile	Amazon EC2	Proteção contra malware EBS	Varia de acordo com a ameaça detectada
Execution:ECS/MaliciousFile	ECS	Proteção contra malware EBS	Varia de acordo com a ameaça detectada

Tipo de descoberta	Tipo de atributo	Dados fundamentais source/Feature	Gravidade da descoberta
Execution:ECS/SuspiciousFile	ECS	Proteção contra malware EBS	Varia de acordo com a ameaça detectada
Execution:Kubernetes/MaliciousFile	Kubernetes	Proteção contra malware EBS	Varia de acordo com a ameaça detectada
Execution:Kubernetes/SuspiciousFile	Kubernetes	Proteção contra malware EBS	Varia de acordo com a ameaça detectada
Execution:EC2/MaliciousFile!Snapshot	Amazon EBS	Proteção contra Malware para Backup	Varia de acordo com a ameaça detectada
Execution:EC2/MaliciousFile!AMI	Amazon EC2	Proteção contra Malware para Backup	Varia de acordo com a ameaça detectada
Execution:EC2/MaliciousFile!RecoveryPoint	AWS Backup	Proteção contra Malware para Backup	Varia de acordo com a ameaça detectada
Execution:S3/MaliciousFile!RecoveryPoint	AWS Backup	Proteção contra Malware para Backup	Varia de acordo com a ameaça detectada
Object:S3/MaliciousFile	S3Object	Proteção contra malware para S3	Alto
CredentialAccess:RDS/AnomalousBehavior.FailedLogin	Bancos de dados do Amazon Aurora, Amazon RDS e Aurora Limitless Databases compatíveis	Monitoramento da atividade de login do RDS	Baixo

Tipo de descoberta	Tipo de atributo	Dados fundamentais source/Feature	Gravidade da descoberta
CredentialAccess:RDS/AnomalousBehavior.SuccessfulBruteForce	Bancos de dados do Amazon Aurora, Amazon RDS e Aurora Limitless Databases compatíveis	Monitoramento da atividade de login do RDS	Alto
CredentialAccess:RDS/AnomalousBehavior.SuccessfulLogin	Bancos de dados do Amazon Aurora, Amazon RDS e Aurora Limitless Databases compatíveis	Monitoramento da atividade de login do RDS	Variável *
CredentialAccess:RDS/MaliciousIPCaller.FailedLogin	Bancos de dados do Amazon Aurora, Amazon RDS e Aurora Limitless Databases compatíveis	Monitoramento da atividade de login do RDS	Médio
CredentialAccess:RDS/MaliciousIPCaller.SuccessfulLogin	Bancos de dados do Amazon Aurora, Amazon RDS e Aurora Limitless Databases compatíveis	Monitoramento da atividade de login do RDS	Alto
CredentialAccess:RDS/TorIPCaller.FailedLogin	Bancos de dados do Amazon Aurora, Amazon RDS e Aurora Limitless Databases compatíveis	Monitoramento da atividade de login do RDS	Médio

Tipo de descoberta	Tipo de atributo	Dados fundamentais source/Feature	Gravidade da descoberta
CredentialAccess:RDS/TorIPCaller.SuccessfulLogin	Bancos de dados do Amazon Aurora, Amazon RDS e Aurora Limitless Databases compatíveis	Monitoramento da atividade de login do RDS	Alto
Discovery:RDS/MaliciousIPCaller	Bancos de dados do Amazon Aurora, Amazon RDS e Aurora Limitless Databases compatíveis	Monitoramento da atividade de login do RDS	Médio
Discovery:RDS/TorIPCaller	Bancos de dados do Amazon Aurora, Amazon RDS e Aurora Limitless Databases compatíveis	Monitoramento da atividade de login do RDS	Médio
Exfiltration:RDS/AnomalousBehavior	Bancos de dados do Amazon Aurora, Amazon RDS e Aurora Limitless Databases compatíveis	Monitoramento de atividades do RDS DB	Baixo *
Exfiltration:RDS/MaliciousIPCaller	Bancos de dados do Amazon Aurora, Amazon RDS e Aurora Limitless Databases compatíveis	Monitoramento de atividades do RDS DB	Alto

Tipo de descoberta	Tipo de atributo	Dados fundamentais source/Feature	Gravidade da descoberta
Exfiltration:RDS/TorIPCaller	Bancos de dados do Amazon Aurora, Amazon RDS e Aurora Limitless Databases compatíveis	Monitoramento de atividades do RDS DB	Alto
Impact:RDS/AnomalousBehavior.Delete	Bancos de dados do Amazon Aurora, Amazon RDS e Aurora Limitless Databases compatíveis	Monitoramento de atividades do RDS DB	Baixo *
Impact:RDS/AnomalousBehavior.Drop	Bancos de dados do Amazon Aurora, Amazon RDS e Aurora Limitless Databases compatíveis	Monitoramento de atividades do RDS DB	Médio *
Impact:RDS/MaliciousIPCaller	Bancos de dados do Amazon Aurora, Amazon RDS e Aurora Limitless Databases compatíveis	Monitoramento de atividades do RDS DB	Alto
Impact:RDS/TorIPCaller	Bancos de dados do Amazon Aurora, Amazon RDS e Aurora Limitless Databases compatíveis	Monitoramento de atividades do RDS DB	Alto

Tipo de descoberta	Tipo de atributo	Dados fundamentais source/Feature	Gravidade da descoberta
Discovery:S3/AnomalousBehavior	Amazon S3	CloudTrail eventos de dados para S3	Baixo
Discovery:S3/MaliciousIPCaller	Amazon S3	CloudTrail eventos de dados para S3	Alto
Discovery:S3/MaliciousIPCaller.Custom	Amazon S3	CloudTrail eventos de dados para S3	Alto
Discovery:S3/TorIPCaller	Amazon S3	CloudTrail eventos de dados para S3	Médio
Exfiltration:S3/AnomalousBehavior	Amazon S3	CloudTrail eventos de dados para S3	Alto
Exfiltration:S3/MaliciousIPCaller	Amazon S3	CloudTrail eventos de dados para S3	Alto
Impact:S3/AnomalousBehavior.Delete	Amazon S3	CloudTrail eventos de dados para S3	Alto
Impact:S3/AnomalousBehavior.Permission	Amazon S3	CloudTrail eventos de dados para S3	Alto
Impact:S3/AnomalousBehavior.Write	Amazon S3	CloudTrail eventos de dados para S3	Médio
Impact:S3/MaliciousIPCaller	Amazon S3	CloudTrail eventos de dados para S3	Alto
PenTest:S3/KaliLinux	Amazon S3	CloudTrail eventos de dados para S3	Médio
PenTest:S3/ParrotLinux	Amazon S3	CloudTrail eventos de dados para S3	Médio

Tipo de descoberta	Tipo de atributo	Dados fundamentais source/Feature	Gravidade da descoberta
PenTest:S3/PentooLinux	Amazon S3	CloudTrail eventos de dados para S3	Médio
UnauthorizedAccess:S3/TorIPCaller	Amazon S3	CloudTrail eventos de dados para S3	Alto
UnauthorizedAccess:S3/MaliciousIPCaller.Custom	Amazon S3	CloudTrail eventos de dados para S3	Alto
Backdoor:Runtime/C&CActivity.B	Instância, cluster EKS, cluster ECS ou contêiner	Monitoramento de runtime	Alto
Backdoor:Runtime/C&CActivity.B!DNS	Instância, cluster EKS, cluster ECS ou contêiner	Monitoramento de runtime	Alto
CryptoCurrency:Runtime/BitcoinTool.B	Instância, cluster EKS, cluster ECS ou contêiner	Monitoramento de runtime	Alto
CryptoCurrency:Runtime/BitcoinTool.B!DNS	Instância, cluster EKS, cluster ECS ou contêiner	Monitoramento de runtime	Alto
DefenseEvasion:Runtime/FilelessExecution	Instância, cluster EKS, cluster ECS ou contêiner	Monitoramento de runtime	Médio
DefenseEvasion:Runtime/KernelModuleLoaded	Instância, cluster EKS, cluster ECS ou contêiner	Monitoramento de runtime	Alto

Tipo de descoberta	Tipo de atributo	Dados fundamentais source/Feature	Gravidade da descoberta
DefenseEvasion:Runtime/SensitiveFileModified	Instância, cluster EKS, cluster ECS ou contêiner	Monitoramento de runtime	Médio
DefenseEvasion:Runtime/ProcessInjection.Proc	Instância, cluster EKS, cluster ECS ou contêiner	Monitoramento de runtime	Alto
DefenseEvasion:Runtime/ProcessInjection.Ptrace	Instância, cluster EKS, cluster ECS ou contêiner	Monitoramento de runtime	Médio
DefenseEvasion:Runtime/ProcessInjection.VirtualMemoryWrite	Instância, cluster EKS, cluster ECS ou contêiner	Monitoramento de runtime	Alto
DefenseEvasion:Runtime/PtraceAntiDebugging	Instância, cluster EKS, cluster ECS ou contêiner	Monitoramento de runtime	Baixo
DefenseEvasion:Runtime/SuspiciousCommand	Instância, cluster EKS, cluster ECS ou contêiner	Monitoramento de runtime	Alto
Discovery:Runtime/SuspiciousCommand	Instância, cluster EKS, cluster ECS ou contêiner	Monitoramento de runtime	Baixo
Execution:Runtime/MaliciousFileExecuted	Instância, cluster EKS, cluster ECS ou contêiner	Monitoramento de runtime	Alto
Execution:Runtime/MaliciousFileExecuted.Custom	Instância, cluster EKS, cluster ECS ou contêiner	Monitoramento de runtime	Alto

Tipo de descoberta	Tipo de atributo	Dados fundamentais source/Feature	Gravidade da descoberta
Execution:Runtime/NewBinaryExecuted	Instância, cluster EKS, cluster ECS ou contêiner	Monitoramento de runtime	Médio
Execution:Runtime/NewLibraryLoaded	Instância, cluster EKS, cluster ECS ou contêiner	Monitoramento de runtime	Médio
Execution:Runtime/SuspiciousCommand	Instância, cluster EKS, cluster ECS ou contêiner	Monitoramento de runtime	Variável
Execution:Runtime/SuspiciousShellCreated	Instância, cluster EKS, cluster ECS ou contêiner	Monitoramento de runtime	Baixo
Execution:Runtime/SuspiciousTool	Instância, cluster EKS, cluster ECS ou contêiner	Monitoramento de runtime	Variável
Execution:Runtime/ReverseShell	Instância, cluster EKS, cluster ECS ou contêiner	Monitoramento de runtime	Alto
Impact:Runtime/AbusedDomainRequest.Reputation	Instância, cluster EKS, cluster ECS ou contêiner	Monitoramento de runtime	Médio
Impact:Runtime/BitcoinDomainRequest.Reputation	Instância, cluster EKS, cluster ECS ou contêiner	Monitoramento de runtime	Alto
Impact:Runtime/CryptoMinerExecuted	Instância, cluster EKS, cluster ECS ou contêiner	Monitoramento de runtime	Alto

Tipo de descoberta	Tipo de atributo	Dados fundamentais source/Feature	Gravidade da descoberta
Impact:Runtime/MaliciousDomainRequest.Reputation	Instância, cluster EKS, cluster ECS ou contêiner	Monitoramento de runtime	Médio
Impact:Runtime/SuspiciousDomainRequest.Reputation	Instância, cluster EKS, cluster ECS ou contêiner	Monitoramento de runtime	Baixo
Persistence:Runtime/SuspiciousCommand	Instância, cluster EKS, cluster ECS ou contêiner	Monitoramento de runtime	Médio
Persistence:Runtime/SensitiveFileModified	Instância, cluster EKS, cluster ECS ou contêiner	Monitoramento de runtime	Médio
PrivilegeEscalation:Runtime/CGroupsReleaseAgentModified	Instância, cluster EKS, cluster ECS ou contêiner	Monitoramento de runtime	Alto
PrivilegeEscalation:Runtime/ContainerMountsHostDirectory	Instância, cluster EKS, cluster ECS ou contêiner	Monitoramento de runtime	Médio
PrivilegeEscalation:Runtime/DockerSocketAccessed	Instância, cluster EKS, cluster ECS ou contêiner	Monitoramento de runtime	Médio
PrivilegeEscalation:Runtime/ElevationToRoot	Instância, cluster EKS, cluster ECS ou contêiner	Monitoramento de runtime	Médio
PrivilegeEscalation:Runtime/RuncContainerEscape	Instância, cluster EKS, cluster ECS ou contêiner	Monitoramento de runtime	Alto

Tipo de descoberta	Tipo de atributo	Dados fundamentais source/Feature	Gravidade da descoberta
PrivilegeEscalation:Runtime/SuspiciousCommand	Instância, cluster EKS, cluster ECS ou contêiner	Monitoramento de runtime	Médio
PrivilegeEscalation:Runtime/SensitiveFileModified	Instância, cluster EKS, cluster ECS ou contêiner	Monitoramento de runtime	Médio
PrivilegeEscalation:Runtime/UserfaultfdUsage	Instância, cluster EKS, cluster ECS ou contêiner	Monitoramento de runtime	Médio
Trojan:Runtime/BlackholeTraffic	Instância, cluster EKS, cluster ECS ou contêiner	Monitoramento de runtime	Médio
Trojan:Runtime/BlackholeTraffic! DNS	Instância, cluster EKS, cluster ECS ou contêiner	Monitoramento de runtime	Médio
Trojan:Runtime/DropPoint	Instância, cluster EKS, cluster ECS ou contêiner	Monitoramento de runtime	Médio
Trojan:Runtime/DGADomainRequest.C! DNS	Instância, cluster EKS, cluster ECS ou contêiner	Monitoramento de runtime	Alto
Trojan:Runtime/DriveBySourceTraffic! DNS	Instância, cluster EKS, cluster ECS ou contêiner	Monitoramento de runtime	Alto
Trojan:Runtime/DropPoint! DNS	Instância, cluster EKS, cluster ECS ou contêiner	Monitoramento de runtime	Médio

Tipo de descoberta	Tipo de atributo	Dados fundamentais source/Feature	Gravidade da descoberta
Trojan:Runtime/PhishingDomainRequest! DNS	Instância, cluster EKS, cluster ECS ou contêiner	Monitoramento de runtime	Alto
UnauthorizedAccess:Runtime/MetadataDNSRebind	Instância, cluster EKS, cluster ECS ou contêiner	Monitoramento de runtime	Alto
UnauthorizedAccess:Runtime/TorClient	Instância, cluster EKS, cluster ECS ou contêiner	Monitoramento de runtime	Alto
UnauthorizedAccess:Runtime/TorRelay	Instância, cluster EKS, cluster ECS ou contêiner	Monitoramento de runtime	Alto

Entendendo e gerando GuardDuty descobertas da Amazon

Uma GuardDuty descoberta representa um possível problema de segurança detectado nas Contas da AWS cargas de trabalho e nos dados. GuardDuty gera uma descoberta sempre que detecta atividades inesperadas e potencialmente maliciosas em seu AWS ambiente.

Você pode visualizar e gerenciar suas GuardDuty descobertas na página Descobertas no GuardDuty console ou usando as operações da API AWS CLI ou. Para obter informações sobre como você pode gerenciar GuardDuty descobertas, consulteGerenciando as GuardDuty descobertas da Amazon.

Tópicos:

GuardDuty formato de busca

Entenda o formato de GuardDuty encontrar os tipos e as diferentes finalidades de ameaças que GuardDuty rastreiam.

Amostras de descobertas

Gere amostras de descobertas no GuardDuty console ou usando a GuardDuty API ou AWS CLI os comandos. As amostras de descobertas geradas incluem detalhes fictícios para ajudar você a entender os detalhes da descoberta associados a cada GuardDuty descoberta. Essas descobertas são marcadas com um prefixo de [AMOSTRA].

GuardDuty Resultados do teste em contas dedicadas

Você pode testar GuardDuty descobertas específicas em seu ambiente. Execute `guardduty-tester` o script em uma não-produção Conta da AWS específica. GuardDuty Para detectar e simular descobertas, ele implantará determinados recursos em seu ambiente. Essa experiência é diferente de gerar descobertas de amostras.

Visualizando as descobertas geradas no GuardDuty console

Saiba como analisar as descobertas geradas no GuardDuty console.

Níveis de severidade das GuardDuty descobertas

Cada GuardDuty descoberta tem um nível de severidade associado que reflete o risco potencial em seu AWS ambiente. Esta seção explica o que cada nível de gravidade significa.

Detalhes da descoberta

Saiba mais sobre os detalhes associados às GuardDuty descobertas que são geradas em sua conta. Este tópico inclui os detalhes associados à detecção básica de ameaças, à detecção estendida de ameaças e aos planos de proteção dedicados em GuardDuty.

GuardDuty encontrando agregação

Saiba como GuardDuty lidar com várias ocorrências do mesmo tipo de descoberta. Ao agregar os mesmos tipos de descoberta detectados, GuardDuty atualiza o tipo de descoberta original com os detalhes mais recentes.

GuardDuty tipos de descoberta

Esta seção lista os tipos de GuardDuty busca por meio do associado Fontes de dados fundamentais ouRecurso mapeado GuardDuty. Para saber mais sobre cada tipo de descoberta, selecione essa descoberta para obter mais detalhes, como sua descrição e possíveis etapas para corrigir a descoberta.

GuardDuty formato de busca

Quando GuardDuty detecta um comportamento suspeito ou inesperado em seu AWS ambiente, ele gera uma descoberta. Uma descoberta é uma notificação que contém os detalhes sobre um possível problema de segurança GuardDuty descoberto. Visualizando as descobertas geradas no GuardDuty consoleIncluem informações sobre o que aconteceu, quais AWS recursos estavam envolvidos na atividade suspeita, quando essa atividade ocorreu e informações relacionadas que podem ajudar você a entender a causa raiz.

Uma das informações mais úteis nos detalhes de descoberta é um tipo de descoberta. O objetivo do tipo de descoberta é fornecer uma descrição concisa e legível do possível problema de segurança. Por exemplo, o tipo de GuardDuty Recon:EC2/PortProbeUnprotectedPortdescoberta informa rapidamente que, em algum lugar do seu AWS ambiente, uma instância do EC2 tem uma porta desprotegida que um invasor em potencial está investigando.

GuardDuty usa o seguinte formato para nomear os vários tipos de descobertas que ele gera:

ThreatPurpose:ResourceTypeAffected/ThreatFamilyName.DetectionMechanism! Artifato

Cada parte desse formato representa um aspecto de um tipo de descoberta. Esses aspectos têm as seguintes explicações:

- ThreatPurpose- descreve o objetivo principal de uma ameaça, um tipo de ataque ou um estágio de um possível ataque. Consulte a seção a seguir para obter uma lista completa das finalidades de GuardDuty ameaças.
- ResourceTypeAffected- descreve qual tipo de AWS recurso é identificado nesta descoberta como o alvo potencial de um adversário. Atualmente, GuardDuty pode gerar descobertas para os tipos de recursos listados noGuardDuty tipos de descoberta ativa.
- ThreatFamilyName- descreve a ameaça geral ou a potencial atividade maliciosa que GuardDuty está sendo detectada. Por exemplo, um valor de NetworkPortUnusualindica que uma instância do EC2 identificada na GuardDuty descoberta não tem histórico anterior de comunicações em uma porta remota específica que também está identificada na descoberta.
- DetectionMechanism- descreve o método no qual GuardDuty detectou a descoberta. Isso pode ser usado para indicar uma variação em um tipo de descoberta comum ou uma descoberta que GuardDuty usou um mecanismo específico para detectar. Por exemplo, Backdoor:EC2/DenialOfService.Tcpindica que a negação de serviço (DoS) foi detectada por TCP. A variante UDP é Backdoor:EC2/DenialOfService.Udp.

  Um valor de .Custom indica que GuardDuty detectou a descoberta com base em suas listas de ameaças personalizadas. Para obter mais informações, consulte Listas de entidades e listas de endereços IP.

  Um valor de .Reputation indica que GuardDuty detectou a descoberta usando um modelo de pontuação de reputação de domínio. Para obter mais informações, consulte Como AWS rastreia as maiores ameaças à segurança da nuvem e ajuda a eliminá-las.
- Artefato: descreve um recurso específico que pertence a uma ferramenta usada no ataque. Por exemplo, o DNS no tipo de descoberta CryptoCurrency:EC2/BitcoinTool.B!DNS indica que uma instância do Amazon EC2 está se comunicando com um domínio conhecido. Bitcoin-related

> **Note**
>
> O artefato é opcional e pode não estar disponível para todos os tipos de GuardDuty descoberta.

OBJETIVO DA AMEAÇA

Em GuardDuty uma ameaça, o propósito descreve o objetivo principal de uma ameaça, um tipo de ataque ou um estágio de um possível ataque. Por exemplo, alguns propósitos de ameaça, como

Backdoor, indicam um tipo de ataque. No entanto, alguns propósitos de ameaça, como Impact, estão alinhados às táticas do MITRE ATT&CK. As táticas do MITRE ATT&CK indicam diferentes fases no ciclo de ataque de um adversário. Na versão atual do GuardDuty, ThreatPurpose pode ter os seguintes valores:

Backdoor

Esse valor indica que um adversário comprometeu um AWS recurso e alterou o recurso para que seja capaz de entrar em contato com seu servidor de comando e controle (C&C) doméstico para receber mais instruções sobre atividades maliciosas.

Comportamento

Esse valor indica que GuardDuty detectou atividade ou padrões de atividade diferentes da linha de base estabelecida para os AWS recursos envolvidos.

CredentialAccess

Esse valor indica que GuardDuty detectou padrões de atividade que um adversário pode usar para roubar credenciais, como senhas, nomes de usuário e chaves de acesso, do seu ambiente. Esse propósito de ameaça é baseado nas táticas do MITRE ATT&CK.

Criptomoedas

Esse valor indica que GuardDuty foi detectado que um AWS recurso em seu ambiente está hospedando software associado a criptomoedas (por exemplo, Bitcoin).

DefenseEvasion

Esse valor indica que GuardDuty detectou atividade ou padrões de atividade que um adversário pode usar para evitar a detecção ao se infiltrar em seu ambiente. O propósito dessa ameaça é baseado nas táticas do MITRE ATT&CK

Descoberta

Esse valor indica que GuardDuty detectou atividade ou padrões de atividade que um adversário pode usar para expandir seu conhecimento sobre seus sistemas e redes internas. Esse propósito de ameaça é baseado nas táticas do MITRE ATT&CK.

Execução

Esse valor indica que GuardDuty detectou que um adversário pode tentar executar ou já executou um código malicioso para explorar o AWS ambiente ou roubar dados. Esse propósito de ameaça é baseado nas táticas do MITRE ATT&CK.

Exfiltration

Esse valor indica que GuardDuty detectou atividade ou padrões de atividade que um adversário pode usar ao tentar roubar dados do seu ambiente. Esse propósito de ameaça é baseado nas táticas do MITRE ATT&CK.

Impacto

Esse valor indica que GuardDuty detectou atividade ou padrões de atividade que sugerem que um adversário está tentando manipular, interromper ou destruir seus sistemas e dados. Esse propósito de ameaça é baseado nas táticas do MITRE ATT&CK.

InitialAccess

Este valor é comumente associado ao estágio inicial de acesso de um ataque, quando um adversário está tentando estabelecer acesso ao seu ambiente. Esse propósito de ameaça é baseado nas táticas do MITRE ATT&CK.

Teste de penetração

Às vezes, proprietários de AWS recursos ou seus representantes autorizados intencionalmente executam testes em AWS aplicativos para encontrar vulnerabilidades, como grupos de segurança abertos ou chaves de acesso que são excessivamente permissivas. Esses testes de penetração são feitos na tentativa de identificar e bloquear recursos vulneráveis antes que eles sejam descobertos por invasores. No entanto, algumas das ferramentas usadas por testadores de penetração autorizados estão disponíveis gratuitamente e podem ser usadas por usuários não autorizados ou invasores para executar testes de sondagem. Embora não GuardDuty consiga identificar o verdadeiro propósito por trás dessa atividade, o valor do Pentest indica que GuardDuty está detectando essa atividade, que ela é semelhante à atividade gerada por ferramentas conhecidas de teste de caneta e que pode indicar uma sondagem maliciosa de sua rede.

Persistência

Esse valor indica que GuardDuty detectou atividades ou padrões de atividade que um adversário pode usar para tentar manter o acesso aos seus sistemas, mesmo que sua rota de acesso inicial seja cortada. Por exemplo, isso pode incluir a criação de um novo usuário do IAM após obter acesso por meio das credenciais comprometidas de um usuário existente. Quando as credenciais do usuário existente forem excluídas, o adversário manterá o acesso ao novo usuário que não foi detectado como parte do evento original. Esse propósito de ameaça é baseado nas táticas do MITRE ATT&CK.

Política

Esse valor indica que você Conta da AWS está exibindo um comportamento que vai contra as melhores práticas de segurança recomendadas. Por exemplo, a modificação não intencional de políticas de permissão associadas aos seus recursos AWS ou ambiente e o uso de contas privilegiadas que deveriam ter pouco ou nenhum uso.

PrivilegeEscalation

Esse valor informa que a entidade principal envolvida em seu ambiente da AWS está exibindo um comportamento que um adversário pode usar para obter permissões de nível superior para sua rede. Esse propósito de ameaça é baseado nas táticas do MITRE ATT&CK.

Recon

Esse valor indica que GuardDuty detectou atividades ou padrões de atividade que um adversário pode usar ao realizar o reconhecimento de seu ambiente para determinar como ele pode ampliar seu acesso ou utilizar seus recursos. Por exemplo, essa atividade pode incluir a análise de vulnerabilidades em seu ambiente da AWS examinando portas, fazendo chamadas de API, listando usuários, tabelas de banco de dados e assim por diante.

Stealth

Esse valor indica que um adversário está ativamente tentando esconder suas ações. Por exemplo, eles podem usar um servidor proxy anônimo, tornando extremamente difícil avaliar a verdadeira natureza da atividade.

Trojan

Esse valor indica que um ataque está usando programas de Trojan que realizam atividades mal-intencionadas silenciosas. Às vezes, esse software assume a aparência de um programa legítimo. Às vezes, os usuários executam esse software acidentalmente. Outras vezes, esse software pode ser executado automaticamente por meio da exploração de uma vulnerabilidade.

UnauthorizedAccess

Esse valor indica que GuardDuty está detectando uma atividade suspeita ou um padrão de atividade suspeita por uma pessoa não autorizada.

GuardDuty mecanismo de verificação de detecção de malware

GuardDuty A Amazon tem um mecanismo de verificação criado e gerenciado internamente e um fornecedor terceirizado. Ambos usam indicadores de comprometimento (IoCs) provenientes de vários

feeds internos que têm visibilidade sobre os diferentes tipos de malware que podem ser alvos. AWS GuardDuty também tem definições de detecção baseadas nas regras da YARA adicionadas por nossos engenheiros de segurança e detecções baseadas em modelos heurísticos e de aprendizado de máquina (ML). Ao escanear objetos do Amazon S3, o GuardDuty Malware Protection produz resultados consistentes ao escanear o mesmo objeto várias vezes com as mesmas definições e mecanismos de escaneamento. Signature-based a detecção não inclui apenas a correspondência de bytes, mas também um trecho de código potencialmente complexo, e o scanner pode analisar o conteúdo e tomar decisões.

O mecanismo de verificação de malware não realiza análise comportamental em tempo real, em que a detonação de malware monitora a amostra à medida que ela é executada em um sistema real. A GuardDuty solução é principalmente uma detecção baseada em arquivos. Para detectar malware sem arquivos, GuardDuty fornece uma solução baseada em agente, como para Monitoramento de runtime Amazon EKS, Amazon EC2 e Amazon ECS (inclusive). AWS Fargate

Sem restrições nos formatos de arquivo que GuardDuty verificam a existência de malware, os mecanismos de verificação que ele usa podem detectar diferentes tipos de malware, como criptomineradores, ransomware e webshells. O mecanismo de GuardDuty verificação totalmente gerenciado atualiza continuamente a lista de assinaturas de malware a cada 15 minutos.

O mecanismo de verificação faz parte do sistema de inteligência de GuardDuty ameaças que usa um componente interno de detonação de malware. Isso gera uma nova inteligência sobre ameaças ao coletar independentemente amostras de malware e benignas de várias fontes. O tipo IoC de hash de arquivo do sistema de inteligência contra ameaças alimenta ainda mais o mecanismo de verificação de malware para detectar os malwares com base em hashes de arquivos inválidos conhecidos.

Gerando descobertas de amostras em GuardDuty

GuardDuty A Amazon ajuda você a gerar amostras de descobertas para visualizar e entender os vários tipos de descobertas que ela pode gerar. Quando você gera amostras de descobertas, GuardDuty preenche sua lista de descobertas atuais com uma amostra para cada tipo de descoberta compatível, incluindo os tipos de descoberta de sequência de ataque.

As amostras geradas são aproximações preenchidas com valores de espaço reservado. Essas amostras podem parecer diferentes das descobertas reais do seu ambiente, mas você pode usá-las para testar várias configurações GuardDuty, como seus EventBridge eventos ou filtros. Para obter uma lista dos valores disponíveis para tipos de descoberta, consulte a tabela GuardDuty tipos de descoberta.

Geração de amostras de descobertas por meio do GuardDuty console ou da API

Selecione seu método de acesso preferido para gerar descobertas de amostra.

> **Note**
>
> O GuardDuty console ajuda você a gerar um de cada tipo de descoberta. Para gerar um ou mais tipos de descoberta específicos, execute as API/CLI etapas associadas.

Console

Use o procedimento a seguir para gerar descobertas de amostra. Esse processo gera uma amostra de descoberta para cada tipo de GuardDuty descoberta.

1. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.
2. No painel de navegação, selecione Configurações.
3. Na página Configurações, em Amostras de descobertas, escolha Gerar amostras de descobertas.
4. No painel de navegação, selecione Descobertas. As descoberta de amostra são exibidas na página Descobertas atuais com o prefixo [SAMPLE].

API/CLI

Você pode gerar uma única amostra de descoberta correspondente a qualquer um dos tipos de GuardDuty descoberta por meio da CreateSampleFindings API. Os valores disponíveis para os tipos de descoberta estão listados na GuardDuty tipos de descoberta tabela.

Isso é útil para testar regras de CloudWatch eventos ou automação com base nas descobertas. O exemplo a seguir mostra como gerar uma descoberta de amostra única do tipo `Backdoor:EC2/DenialOfService.Tcp` usando a AWS CLI.

Para encontrar o da `detectorId` sua conta e da região atual, consulte a página Configurações no https://console.aws.amazon.com/guardduty/ console ou execute a ListDetectors API.

```
aws guardduty create-sample-findings --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --finding-types Backdoor:EC2/DenialOfService.Tcp
```

O título das descobertas de amostra geradas por meio de algum desses métodos sempre começa com [SAMPLE] no console. As descobertas de amostra têm um valor de `"sample": true` na seção additionalInfo dos detalhes do JSON de descoberta.

Para entender os detalhes da descoberta, como a gravidade da descoberta e o recurso potencialmente comprometido, associados às descobertas geradas, consulte Níveis de severidade das GuardDuty descobertas e Detalhes da descoberta.

Para gerar algumas descobertas comuns com base em uma atividade simulada em um ambiente dedicado e isolado Conta da AWS em seu ambiente, consulteGuardDuty Resultados do teste em contas dedicadas.

GuardDuty Resultados do teste em contas dedicadas

Use este documento para executar um script de testador que gera GuardDuty descobertas em relação aos recursos de teste que serão implantados em seu. Conta da AWS Você pode realizar essas etapas quando quiser entender e aprender sobre determinados tipos de GuardDuty descoberta e como os detalhes da descoberta procuram recursos reais em sua conta. Essa experiência é diferente de gerar Amostras de descobertas. Para obter mais informações sobre a experiência de testar GuardDuty os resultados, consulteConsiderações.

Conteúdo

- Considerações
- GuardDuty descobertas que o script do testador pode gerar
- Etapa 1: pré-requisitos
- Etapa 2 - Implantar AWS recursos
- Etapa 3 - Executar scripts do testador
- Etapa 4 - Limpar os recursos AWS de teste
- Solução de problemas comuns do

Considerações

Antes de continuar, leve em conta as seguintes considerações:

- GuardDuty recomenda implantar o testador em um local dedicado que não seja de produção. Conta da AWS Essa abordagem garantirá que você seja capaz de identificar adequadamente GuardDuty as descobertas geradas pelo testador. Além disso, o GuardDuty testador implanta uma variedade de recursos que podem exigir permissões do IAM além das permitidas em outras contas. O uso de uma conta exclusiva garante que as permissões possam ter o escopo adequado com um limite de conta claro.
- O script do testador gera mais de 100 GuardDuty descobertas com diferentes combinações AWS de recursos. Atualmente, isso não inclui todos os GuardDuty tipos de descoberta. Para obter uma lista dos tipos de descoberta que você pode gerar com esse script de testador, consulte GuardDuty descobertas que o script do testador pode gerar.

  > **Observação**
  >
  > Para visualizar os tipos de descoberta da sequência de ataque, o script do testador gera somente AttackSequence:EKS/CompromisedCluster e AttackSequence:S3/CompromisedData. Para visualizar e entender AttackSequence:IAM/CompromisedCredentials, você pode gerar Amostras de descobertas na sua conta.

- Para que o GuardDuty testador funcione conforme o esperado, ele GuardDuty precisa estar habilitado na conta em que os recursos do testador são implantados. Dependendo dos testes que serão executados, o testador avalia se os planos de GuardDuty proteção apropriados estão habilitados ou não. Para qualquer plano de proteção que não esteja habilitado, GuardDuty solicitará permissão para habilitar os planos de proteção necessários por tempo suficiente GuardDuty para realizar os testes que gerarão resultados. Posteriormente, GuardDuty desativará o plano de proteção quando o teste for concluído.

  Ativando GuardDuty pela primeira vez

  Quando GuardDuty for ativada em sua conta dedicada pela primeira vez em uma região específica, sua conta será automaticamente inscrita em um teste gratuito de 30 dias.

  GuardDuty oferece planos de proteção opcionais. No momento da ativação GuardDuty, alguns planos de proteção também são ativados e incluídos no teste gratuito GuardDuty de 30 dias. Para obter mais informações, consulte Usando o GuardDuty teste gratuito de 30 dias.

GuardDuty já está habilitado em sua conta antes de executar o script do testador

Quando já GuardDuty estiver ativado, com base nos parâmetros, o script do testador verificará o status da configuração de determinados planos de proteção e outras configurações no nível da conta necessárias para gerar as descobertas.

Ao executar esse script de teste, determinados planos de proteção podem ser habilitados pela primeira vez em sua conta exclusiva em uma região. Esse procedimento iniciará a avaliação gratuita de 30 dias para esse plano de proteção. Para obter informações sobre o teste gratuito associado a cada plano de proteção, consulte Usando o GuardDuty teste gratuito de 30 dias.

- Desde que a infraestrutura do GuardDuty testador esteja implantada, você poderá ocasionalmente receber UnauthorizedAccess:EC2/TorClient descobertas da PenTest instância.

GuardDuty descobertas que o script do testador pode gerar

Atualmente, o script do testador gera os seguintes tipos de descoberta relacionados aos registros de auditoria do Amazon EC2, do Amazon EKS, Amazon S3, do IAM e logs de auditoria do EKS:

- AttackSequence:EKS/CompromisedCluster
- AttackSequence:S3/CompromisedData
- Backdoor:EC2/C&CActivity.B!DNS
- Backdoor:EC2/DenialOfService.Dns
- Backdoor:EC2/DenialOfService.Udp
- CryptoCurrency:EC2/BitcoinTool.B!DNS
- Impact:EC2/AbusedDomainRequest.Reputation
- Impact:EC2/BitcoinDomainRequest.Reputation
- Impact:EC2/MaliciousDomainRequest.Reputation
- Impact:EC2/SuspiciousDomainRequest.Reputation
- Recon:EC2/Portscan
- Trojan:EC2/BlackholeTraffic!DNS
- Trojan:EC2/DGADomainRequest.C!DNS
- Trojan:EC2/DNSDataExfiltration
- Trojan:EC2/DriveBySourceTraffic!DNS
- Trojan:EC2/DropPoint!DNS

- Trojan:EC2/PhishingDomainRequest!DNS
- UnauthorizedAccess:EC2/MaliciousIPCaller.Custom
- UnauthorizedAccess:EC2/RDPBruteForce
- UnauthorizedAccess:EC2/SSHBruteForce
- PenTest:IAMUser/KaliLinux
- Recon:IAMUser/MaliciousIPCaller.Custom
- Recon:IAMUser/TorIPCaller
- Stealth:IAMUser/CloudTrailLoggingDisabled
- Stealth:IAMUser/PasswordPolicyChange
- UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS
- UnauthorizedAccess:IAMUser/MaliciousIPCaller.Custom
- UnauthorizedAccess:IAMUser/TorIPCaller
- Discovery:Kubernetes/MaliciousIPCaller.Custom
- Discovery:Kubernetes/SuccessfulAnonymousAccess
- Discovery:Kubernetes/TorIPCaller
- Execution:Kubernetes/ExecInKubeSystemPod
- Impact:Kubernetes/MaliciousIPCaller.Custom
- Persistence:Kubernetes/ContainerWithSensitiveMount
- Policy:Kubernetes/AdminAccessToDefaultServiceAccount
- Policy:Kubernetes/AnonymousAccessGranted
- PrivilegeEscalation:Kubernetes/PrivilegedContainer
- UnauthorizedAccess:Lambda/MaliciousIPCaller.Custom
- Discovery:S3/MaliciousIPCaller.Custom
- Discovery:S3/TorIPCaller
- PenTest:S3/KaliLinux
- Policy:S3/AccountBlockPublicAccessDisabled
- Policy:S3/BucketAnonymousAccessGranted
- Policy:S3/BucketBlockPublicAccessDisabled
- Policy:S3/BucketPublicAccessGranted
- Stealth:S3/ServerAccessLoggingDisabled

- UnauthorizedAccess:S3/MaliciousIPCaller.Custom
- UnauthorizedAccess:S3/TorIPCaller
- Backdoor:Runtime/C&CActivity.B! DNS
- CryptoCurrency:Runtime/BitcoinTool.B! DNS
- DefenseEvasion:Runtime/ProcessInjection.Ptrace
- DefenseEvasion:Runtime/ProcessInjection.VirtualMemoryWrite
- Execution:Runtime/ReverseShell
- Impact:Runtime/AbusedDomainRequest.Reputation
- Impact:Runtime/BitcoinDomainRequest.Reputation
- Impact:Runtime/MaliciousDomainRequest.Reputation
- Impact:Runtime/SuspiciousDomainRequest.Reputation
- PrivilegeEscalation:Runtime/ContainerMountsHostDirectory
- PrivilegeEscalation:Runtime/DockerSocketAccessed
- Trojan:Runtime/BlackholeTraffic! DNS
- Trojan:Runtime/DGADomainRequest.C! DNS
- Trojan:Runtime/DriveBySourceTraffic! DNS
- Trojan:Runtime/DropPoint! DNS
- Trojan:Runtime/PhishingDomainRequest! DNS

Etapa 1: pré-requisitos

Para preparar seu ambiente de teste, é preciso ter os seguintes itens:

- Git — Instale a ferramenta de linha de comando git com base no sistema operacional usado.

  Isso é necessário para clonar o `amazon-guardduty-tester`repositório.
- AWS Command Line Interface— Uma ferramenta de código aberto que permite que você interaja Serviços da AWS usando comandos em seu shell de linha de comando. Para obter mais informações, consulte Conceitos básicos do AWS CLI no Manual do usuário do AWS Command Line Interface .
- AWS Systems Manager— Para iniciar sessões do Gerenciador de Sessões com seus nós gerenciados usando, AWS CLI você deve instalar o plug-in do Gerenciador de Sessões em sua

máquina local. Para obter mais informações, consulte Install the Session Manager Plugin for the AWS CLI no Guia do usuário do AWS Systems Manager .

- Node Package Manager (NPM) — Instale o NPM para instalar todas as dependências.
- Docker: é necessário ter o Docker instalado. Para obter instruções de instalação, consulte o site do Docker.

  Para verificar se o Docker foi instalado, execute o comando a seguir e confirme se há uma saída semelhante à seguinte saída:

```
$ docker --version
Docker version 19.03.1
```

- Assine a imagem do Kali Linux no AWS Marketplace.

Etapa 2 - Implantar AWS recursos

Esta seção fornece uma lista dos principais conceitos e as etapas para implantar determinados recursos do AWS em sua conta dedicada.

Conceitos

A lista a seguir fornece os principais conceitos relacionados aos comandos que ajudam a implantar os recursos:

- AWS Cloud Development Kit (AWS CDK)— O CDK é uma estrutura de desenvolvimento de software de código aberto para definir a infraestrutura de nuvem em código e provisioná-la por meio dela. CloudFormation Você pode usar qualquer uma dessas linguagens de programação compatíveis para definir componentes de nuvem reutilizáveis conhecidos como constructos. Você os compõe em pilhas e aplicativos. Em seguida, você pode implantar seus aplicativos CDK CloudFormation para provisionar ou atualizar seus recursos. Para obter mais informações, consulte O que é o AWS CDK? no Guia do AWS Cloud Development Kit (AWS CDK) desenvolvedor.
- Bootstrapping — É o processo de preparar seu AWS ambiente para uso com. AWS CDK Antes de implantar uma pilha de CDK em um AWS ambiente, o ambiente deve primeiro ser inicializado. Esse processo de provisionamento de AWS recursos específicos em seu ambiente que são usados por AWS CDK faz parte das etapas que você executará na próxima seção -. Etapas para implantar AWS recursos

Para obter mais informações sobre inicialização, consulte Inicialização no Guia do desenvolvedor do AWS Cloud Development Kit (AWS CDK) .

Etapas para implantar AWS recursos

Execute as etapas a seguir para começar a implantar os recursos:

1. Configure sua conta e região AWS CLI padrão, a menos que as variáveis de região da conta dedicada sejam definidas manualmente no `bin/cdk-gd-tester.ts` arquivo. Para obter mais informações, consulte Ambientes no Guia do desenvolvedor do AWS Cloud Development Kit (AWS CDK) .
2. Para implantar os recursos, execute os seguintes comandos:

```
git clone https://github.com/awslabs/amazon-guardduty-tester && cd amazon-guardduty-tester
npm install
cdk bootstrap
cdk deploy
```

O último comando (`cdk deploy`) cria uma CloudFormation pilha em seu nome. O nome dessa pilha é GuardDutyTesterStack.

Como parte desse script, GuardDuty cria novos recursos para gerar GuardDuty descobertas em sua conta. Além disso, ele adiciona o seguinte par de tag chave:valor às instâncias do Amazon EC2:

`CreatedBy:GuardDuty Test Script`

As instâncias do Amazon EC2 também incluem as instâncias do EC2 que hospedam nós do EKS e clusters do ECS.

> **Tipos de instância**
>
> GuardDuty foi projetado para usar tipos de instância econômicos que fornecem o desempenho mínimo necessário para realizar testes com êxito. Devido aos requisitos de vCPU, o grupo de nós do Amazon EKS exige `t3.medium`, e, devido ao aumento da capacidade de rede necessária para testes de descoberta de DenialOfService, o nó do driver exige `m6i.large`. Para todos os outros testes, GuardDuty usa o tipo de `t3.micro`

instância. Para obter mais informações sobre os tipos de instância, consulte Tipos de instância no Guia de Tipos de Instâncias do Amazon EC2.

Etapa 3 - Executar scripts do testador

Esse é um processo de duas etapas em que você primeiro precisa iniciar uma sessão com o driver de teste e, em seguida, executar scripts para gerar GuardDuty descobertas com combinações de recursos específicas.

Parte A - Iniciar sessão com o driver de teste

1. Depois que seus recursos forem implantados, salve o código da região em uma variável na sessão atual do terminal. Use o comando a seguir e *us-east-1* substitua pelo código da região em que você implantou os recursos:

   ```
   $ REGION=us-east-1
   ```

2. O script do testador está disponível somente por meio do AWS Systems Manager (SSM). Para iniciar um shell interativo na instância do host do testador, consulte o host InstanceId.
3. Use o comando a seguir para iniciar sua sessão para o script do testador:

   ```
   aws ssm start-session
     --region $REGION
     --document-name AWS-StartInteractiveCommand
     --parameters command="cd /home/ssm-user/py_tester && bash -l"
     --target $(aws ec2 describe-instances
       --region $REGION
       --filters "Name=tag:Name,Values=Driver-GuardDutyTester"
       --query "Reservations[].Instances[?State.Name=='running'].InstanceId"
       --output text)
   ```

Parte B - Gerar descobertas

O script do testador é um Python-based programa que cria dinamicamente um script bash para gerar descobertas com base em sua entrada. Você tem flexibilidade para gerar descobertas com base em um ou mais tipos de AWS recursos, planos de GuardDuty proteção OBJETIVO DA AMEAÇA (táticas) outhe section called “GuardDuty descobertas que o script do testador pode gerar”. Fontes de dados fundamentais

Use os exemplos de comandos a seguir como referência e execute um ou mais comandos para gerar as descobertas que deseja explorar:

```
python3 guardduty_tester.py
python3 guardduty_tester.py --all
python3 guardduty_tester.py --s3
python3 guardduty_tester.py --tactics discovery
python3 guardduty_tester.py --ec2 --eks --tactics backdoor policy execution
python3 guardduty_tester.py --eks --runtime only
python3 guardduty_tester.py --ec2 --runtime only --tactics impact
python3 guardduty_tester.py --log-source dns vpc-flowlogs
python3 guardduty_tester.py --finding 'CryptoCurrency:EC2/BitcoinTool.B!DNS'
```

Para obter mais informações sobre parâmetros válidos, execute o comando de ajuda a seguir:

```
python3 guardduty_tester.py --help
```

Parte C - Analisar as descobertas geradas

Escolha um método de sua preferência para visualizar as descobertas geradas em sua conta.

GuardDuty console

1. Faça login no Console de gerenciamento da AWS e abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.
2. No painel de navegação, selecione Descobertas.
3. Na tabela de descobertas, selecione uma descoberta cujos detalhes deseja visualizar. Isso abrirá o painel de detalhes da descoberta. Para mais informações, consulte Entendendo e gerando GuardDuty descobertas da Amazon.
4. Caso queira filtrar essas descobertas, use a chave e o valor da tag do recurso. Por exemplo, para filtrar as descobertas geradas para as instâncias do Amazon EC2, use**`CreatedBy`**: **`GuardDuty Test Script`** tag key:value pair para Instance tag key e Instance tag key.

API

- Corra ListFindingspara ver as descobertas de um ID de detector específico. É possível usar parâmetros específicos para filtrar as descobertas.

Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no https://console.aws.amazon.com/guardduty/console ou execute a ListDetectorsAPI.

AWS CLI

- Execute o AWS CLI comando a seguir para visualizar as descobertas geradas *us-east-1* e *12abc34d567e8fa901bc2d34EXAMPLE* substituí-las por valores adequados:

```
aws guardduty list-findings --region us-east-1 --detector-
id 12abc34d567e8fa901bc2d34EXAMPLE
```

Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no https://console.aws.amazon.com/guardduty/console ou execute a ListDetectorsAPI.

Para obter mais informações sobre os parâmetros que você pode usar para filtrar descobertas, consulte list-findings na Referência de Comandos AWS CLI .

Etapa 4 - Limpar os recursos AWS de teste

As configurações em nível de conta e outras atualizações de status de configuração feitas durante o retorno Etapa 3 - Executar scripts do testador ao estado original quando o script do testador é concluído.

Depois de executar o script do testador, você pode optar por limpar os recursos de AWS teste. Isso pode ser feito usando um dos seguintes métodos.

- Execute este comando: .

```
cdk destroy
```

- Exclua a CloudFormation pilha com o nome GuardDutyTesterStack. Para obter informações sobre as etapas, consulte Excluindo uma pilha no CloudFormation console.

Solução de problemas comuns do

GuardDuty identificou problemas comuns e recomenda etapas de solução de problemas:

- `Cloud assembly schema version mismatch`— Atualize a AWS CDK CLI para uma versão compatível com a versão de montagem em nuvem necessária ou para a versão mais recente disponível. Para obter mais informações sobre a compatibilidade da CLI AWS CDK.
- `Docker permission denied` – Adicione o usuário da conta exclusiva a docker ou docker-users para que a conta exclusiva possa executar os comandos. Para obter mais informações sobre as etapas, consulte a opção de soquete Daemon.
- `Your requested instance type is not supported in your requested Availability Zone`— Algumas zonas de disponibilidade não oferecem suporte a tipos específicos de instância. Para identificar quais zonas de disponibilidade oferecem suporte ao seu tipo de instância preferido e tentar implantar AWS recursos novamente, execute as seguintes etapas:

  1. Selecione um método de sua preferência para determinar quais zonas de disponibilidade são compatíveis com seu tipo de instância:

     Console

     Para identificar as zonas de disponibilidade compatíveis com o tipo de instância preferencial

     1. Faça login no Console de gerenciamento da AWS e abra o console do Amazon EC2 em. https://console.aws.amazon.com/ec2/
     2. Ao usar o seletor de AWS região no canto superior direito da página, escolha a região em que você deseja iniciar a instância.
     3. No painel de navegação, em Instâncias, escolha Tipos de Instâncias.
     4. Na tabela Tipos de instância, escolha um tipo de instância preferencial.
     5. Em Rede, veja as regiões listadas em Zonas de disponibilidade.

        Com base nessas informações, talvez seja necessário escolher uma nova região onde se possa implantar os recursos.

     AWS CLI

     Execute o comando a seguir para visualizar uma lista de zonas de disponibilidade. Certifique-se de especificar o tipo de instância de sua preferência e a região (*`us-east-1`*).

```
aws ec2 describe-instance-type-offerings --location-type availability-zone  --
filters Name=instance-type,Values=Preferred instance type --region us-east-1 --
output table
```

Para obter mais informações, consulte describe-instance-type-offerings na Referência de comando AWS CLI .

Ao executar esse comando, se você receber um erro, verifique se está usando a versão mais recente da AWS CLI. Para obter mais informações, consulte Troubleshooting no Guia do usuário do AWS Command Line Interface .

2. Tente implantar os AWS recursos novamente e especifique uma zona de disponibilidade compatível com seu tipo de instância preferido.

   Para tentar implantar AWS recursos novamente

   1. Configure a região padrão no arquivo `bin/cdk-gd-tester.ts`.
   2. Para especificar a zona de disponibilidade, abra o arquivo `amazon-guardduty-tester/lib/common/network/vpc.ts`.
   3. Nesse arquivo, substitua `maxAzs: 2,` por `availabilityZones: ['us-east-1a', 'us-east-1c'],` onde você deve especificar as zonas de disponibilidade para seu tipo de instância.
   4. Continue com as etapas restantes em Etapas para implantar AWS recursos.

Visualizando as descobertas geradas no GuardDuty console

Quando GuardDuty detecta uma atividade que corresponde ao padrão de um problema de segurança, GuardDuty gera uma descoberta. Esse tipo de descoberta está associado a um tipo de recurso que pode ter sido comprometido durante essa atividade. Você pode visualizar os detalhes associados a cada descoberta GuardDuty gerada.

Se você estiver usando uma conta de GuardDuty administrador, poderá visualizar as descobertas geradas em nome das contas dos membros. No entanto, uma conta-membro só pode visualizar as descobertas geradas em sua própria conta. Uma conta de membro não pode ver as descobertas geradas para outras contas de membros.

Etapas para visualizar as descobertas no GuardDuty console

1. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.
2. No painel de navegação à esquerda, escolha Descobertas.

   GuardDuty exibe as descobertas em formato tabular. Por padrão, essa tabela é classificada em ordem decrescente com base no valor da coluna Visto pela última vez, exibindo as descobertas mais recentes na parte superior.

   As descobertas com um ícone de espada

   ()

   representam uma descoberta de sequência de ataque.
3. Para ver os detalhes associados a uma descoberta, selecione seu título. Isso abrirá o painel lateral de detalhes da descoberta. Para encontrar uma sequência de ataque, esse painel lateral inclui uma versão resumida da sequência de ataque e, para expandir essa exibição, escolha Exibir detalhes.

   Para obter informações sobre os campos listados nesse painel lateral, consulte Detalhes da descoberta.
4. (Opcional) para baixar o JSON de descoberta

   a. Selecione a descoberta e escolha o menu Ações.

   b. No menu Ações, escolha Exibir e exportar JSON.

   c. Na janela JSON de descobertas, escolha Baixar.

> **Note**
>
> Em alguns casos, GuardDuty percebe que certas descobertas são falsos positivos após serem geradas. GuardDuty fornece um campo Confiança no JSON da descoberta e define seu valor como zero. GuardDuty Dessa forma, você sabe que pode ignorar essas descobertas com segurança.
> Descobertas sem o campo Confiança não são consideradas falsos positivos.

Navegar na página de descobertas

Esta seção fornece informações importantes sobre vários elementos da página Descobertas. Isso ajudará você a analisar as descobertas geradas para análise e resposta a ameaças.

A lista a seguir explica os elementos da página Descobertas que ajudarão você a entender melhor as descobertas geradas:

- Tipo de ameaça:

  O tipo de ameaça inclui GuardDuty descobertas individuais e descobertas de sequências de ataque. Por padrão, a página exibe Todas as descobertas.

  Para filtrar a exibição da tabela de descobertas, no menu Tipo de ameaça, escolha uma das opções: Somente descobertas de sequência de ataque ou Somente descobertas individuais.

- Colunas Recurso e Contagem:

  A coluna Recurso na tabela de descobertas mostra o nome do AWS recurso potencialmente comprometido. Para encontrar uma sequência de ataque, essa coluna mostra o número de AWS recursos potencialmente comprometidos. Para ver os nomes dos recursos, selecione o número na coluna Recurso.

  A coluna Contagem indica o número de vezes que GuardDuty observa uma descoberta específica. Quando GuardDuty detecta uma atividade que corresponde a um problema de segurança identificado anteriormente, ela aumenta a contagem dessa descoberta específica. Para uma descoberta de sequência de ataque, esse valor de coluna indica o número total de sinais e descobertas envolvidos na geração da descoberta.

- Classificando as descobertas por colunas da tabela:

  Se houver uma seta ao lado do cabeçalho da coluna, você poderá classificar a tabela de descobertas com base na coluna. Selecione o cabeçalho da coluna para classificar as descobertas em ordem crescente ou decrescente do valor nessa coluna.

- Filtrar descobertas:

  Com base em atributos de propriedade específicos, como `Account ID` e `Resource type`, você pode filtrar ainda mais a tabela de descobertas. Para obter mais informações sobre os tipos de filtros que você pode usar, consulte Filtrando descobertas GuardDuty .

- Status e regras salvas:

O menu Status inclui dois valores: Atual e Arquivado. A exibição padrão é de descobertas atuais na tabela.

Quando você não quiser mais GuardDuty gerar uma descoberta que corresponda a um critério específico, você pode suprimir essa descoberta. GuardDuty arquiva essa descoberta. Quando GuardDuty detectar essa descoberta novamente, você não será notificado dessa observação. Para visualizar especificamente as descobertas arquivadas, no menu Status, escolha Arquivado.

As regras salvas são um recurso que ajuda você a filtrar e executar ações automaticamente nas descobertas que correspondem a um critério específico. As ações podem incluir arquivar descobertas ou suprimi-las de futuras notificações.

Para obter mais informações, consulte Regras de supressão.

Níveis de severidade das GuardDuty descobertas

Cada GuardDuty descoberta tem um nível de severidade e um valor atribuídos que refletem o risco potencial que a descoberta pode ter para seu ambiente, conforme determinado por nossos engenheiros de segurança. O valor da gravidade pode estar entre 1,0 e 10,0, com valores mais altos indicando maior risco de segurança. Para ajudá-lo a determinar uma resposta a um possível problema de segurança que é destacado por uma descoberta, GuardDuty divide esse intervalo em níveis de gravidade crítico , alto, médio e baixo.

Uma descoberta de um tipo específico pode ter uma gravidade diferente dependendo do contexto específico da descoberta. Para ver uma lista consolidada dos níveis de severidade padrão para todos os tipos de GuardDuty descoberta, consulteGuardDuty tipos de descoberta ativa.

As seções a seguir explicam os níveis de severidade definidos para as GuardDuty descobertas.

Tópicos

- Gravidade crítica
- Gravidade alta
- Gravidade média
- Gravidade baixa

Gravidade crítica

Intervalo de valores: 9,0 – 10,0

Descrição: um nível de gravidade crítica indica que uma sequência de ataque pode estar em andamento ou ter ocorrido recentemente. Um ou mais AWS recursos, como credenciais de login de usuário do IAM e bucket do Amazon S3, estão potencialmente comprometidos ou podem já ter sido comprometidos.

Recomendação: GuardDuty recomenda que você priorize a triagem e a correção de todas as descobertas críticas de gravidade, pois esses problemas podem fazer parte de um ataque de ransomware e aumentar a qualquer momento. Veja detalhes sobre os recursos envolvidos e comece a abordar os problemas de segurança. Para obter mais informações, consulte Correção de descobertas.

Gravidade alta

Intervalo de valores: 7,0 – 8,9

Descrição: um nível de gravidade alta indica que o recurso em questão (uma instância do Amazon EC2 ou um conjunto de credenciais de login de usuário do IAM) está comprometido e sendo usado ativamente para fins não autorizados.

Recomendação: GuardDuty recomenda que você trate qualquer problema de segurança detectado de alta gravidade como uma prioridade e tome medidas imediatas de remediação para evitar o uso não autorizado adicional de seus recursos. Por exemplo, limpe sua instância do Amazon EC2 ou encerre-a, ou mude as credenciais do IAM. Siga as etapas em Correção de descobertas para corrigir a descoberta.

Gravidade média

Intervalo de valores: 4,0 – 6,9

Descrição: um nível de gravidade média indica atividade suspeita que se desvia do comportamento normalmente observado e, dependendo do seu caso de uso, pode indicar o comprometimento de recursos.

Recomendação: GuardDuty recomenda investigar o recurso potencialmente impactado o mais rápido possível. As etapas de correção variam de acordo com o recurso e a família da descoberta. Uma

abordagem estabelecida é confirmar se a atividade está autorizada e é consistente com o caso de uso. Se você não conseguir identificar a causa ou confirmar se a atividade foi autorizada, considere o recurso como comprometido. Siga as etapas em Correção de descobertas para corrigir a descoberta.

Veja alguns itens a serem considerados ao analisar uma descoberta de nível médio:

- Verifique se um usuário autorizado instalou um novo software que alterou o comportamento de um recurso (por exemplo, permitido tráfego superior ao normal ou comunicação habilitada em uma nova porta).
- Verifique se um usuário autorizado alterou as configurações do plano de controle, por exemplo, modificou uma configuração de grupo de segurança.
- Execute uma verificação antivírus no recurso implicado para detectar software não autorizado.
- Verifique as permissões associadas ao perfil, usuário, grupo ou conjunto de credenciais afetados do IAM. Pode ser necessário alterá-las.

Gravidade baixa

Intervalo de valores: 1,0 – 3,9

Descrição: um nível de gravidade baixa indica uma tentativa de atividade suspeita que não comprometeu seu ambiente. Por exemplo, uma varredura de porta ou uma tentativa de invasão fracassada.

Recomendação: não há nenhuma ação recomendada imediata, mas vale a pena anotar essas informações, pois elas podem indicar que alguém está procurando pontos fracos em seu ambiente.

Detalhes da descoberta

No GuardDuty console da Amazon, você pode ver os detalhes da descoberta na seção de resumo da descoberta. Os detalhes da descoberta variam de acordo com o tipo de descoberta.

Há dois detalhes principais que determinarão quais tipos de informações serão disponibilizadas para qualquer descoberta. O primeiro é o tipo de recurso, que pode ser `Instance`, `AccessKey`, `S3Bucket`, `S3Object`, `Kubernetes cluster`, `ECS cluster`, `Container`, `RDSDBInstance`, `RDSLimitlessDB` ou `Lambda`. O segundo detalhe que determina as informações da descoberta é a Função do recurso. A função do recurso pode ser `Target`, o que significa que o recurso foi alvo de atividades suspeitas. Por exemplo, tipo de descoberta, a função do recurso também pode ser `Actor`,

o que significa que seu recurso foi o agente que realizou atividades suspeitas. Este tópico descreve alguns dos detalhes geralmente disponíveis sobre descobertas. Para the section called “Tipos de descoberta do Monitoramento de runtime” eTipo de descoberta da Proteção contra malware para S3, a função do recurso não foi preenchida.

Tópicos

- Visão geral da descoberta
- Recurso
- Detalhes da descoberta da sequência de ataques
- Regras de detecção personalizadas encontrando detalhes
- Detalhes do usuário do banco de dados (DB) do RDS
- Detalhes da descoberta do monitoramento de runtime
- Detalhes de verificação de volumes do EBS
- Detalhes de descobertas sobre a Proteção contra malware para EC2
- Detalhes de descobertas sobre a Proteção contra malware para S3
- Ação
- Agente ou destino
- Detalhes de geolocalização
- Mais informações
- Evidência
- Comportamento anômalo

Visão geral da descoberta

A seção Visão geral de uma descoberta contém os atributos de identificação mais básicos da descoberta, incluindo as seguintes informações:

- ID da conta — A ID da AWS conta na qual a atividade ocorreu que solicitou GuardDuty a geração dessa descoberta.
- Contagem — O número de vezes GuardDuty que agregou uma atividade que corresponde a esse padrão a essa ID de descoberta.
- Criada em: a data e hora em que esta descoberta foi criada pela primeira vez. Se esse valor for diferente de Atualizado em indica que a atividade ocorreu várias vezes e é um problema contínuo.

> **Note**
>
> Os carimbos de data e hora das descobertas no GuardDuty console aparecem em seu fuso horário local, enquanto as exportações JSON e as saídas de CLI exibem carimbos de data e hora em UTC.

- ID da descoberta: um ID exclusivo para este tipo de descoberta e conjunto de parâmetros. Novas ocorrências de atividades que correspondem a esse padrão serão agregadas ao mesmo ID.
- Tipo de descoberta: uma string formatada representando o tipo de atividade que acionou a descoberta. Para obter mais informações, consulte GuardDuty formato de busca.
- Região — A AWS região na qual a descoberta foi gerada. Para obter mais informações sobre as regiões compatíveis, consulte Regiões e endpoints
- ID do recurso — O ID do AWS recurso contra o qual a atividade ocorreu e que solicitou GuardDuty a geração dessa descoberta.
- ID de verificação — Aplicável às descobertas quando a Proteção contra GuardDuty Malware para EC2 está ativada, é um identificador da verificação de malware que é executada nos volumes do EBS conectados à carga de trabalho da instância ou contêiner do EC2 potencialmente comprometida. Para obter mais informações, consulte Detalhes de descobertas sobre a Proteção contra malware para EC2.
- Gravidade: o nível de gravidade atribuído à descoberta, que pode ser Crítica, Alta, Média ou Baixa. Para obter mais informações, consulte Níveis de gravidade das descobertas.
- Atualizado em — A última vez que essa descoberta foi atualizada com uma nova atividade correspondente ao padrão que levou GuardDuty à geração dessa descoberta.

Recurso

O recurso afetado fornece detalhes sobre o AWS recurso que foi alvo da atividade inicial. As informações disponíveis variam de acordo com o tipo de recurso e o tipo de ação.

Função do recurso — A função do AWS recurso que iniciou a descoberta. Esse valor pode ser TARGET ou ACTOR, e representa se seu recurso foi o alvo da atividade suspeita ou o ator que realizou a atividade suspeita, respectivamente.

Tipo de recurso: o tipo de recurso afetado. Se houver vários recursos envolvidos, uma descoberta poderá incluir vários tipos de recursos. Os tipos de recursos são Instance, S3Bucket AccessKey,

S3Object, ECSCluster, Container, RDSDBInstance KubernetesCluster, RDSLimitlessDB e Lambda. Dependendo do tipo de recurso, diferentes detalhes da descoberta estarão disponíveis. Selecione uma guia de opções do recurso para saber mais sobre os detalhes disponíveis para ele.

Instance

Detalhes da instância:

> **Note**
>
> Alguns detalhes da instância podem estar ausentes se a instância já tiver sido interrompida ou se a invocação da API subjacente tiver se originado de uma instância do EC2 em uma região diferente ao fazer uma chamada de API entre regiões.

- ID da instância — A ID da instância do EC2 envolvida na atividade que solicitou GuardDuty a geração da descoberta.
- Tipo de instância: o tipo de instância do EC2 envolvida na descoberta.
- Hora de execução: a data e a hora em que a instância foi executada.
- Outpost ARN — O nome de recurso da Amazon (ARN) de. AWS Outposts Aplicável somente às AWS Outposts instâncias. Para obter mais informações, consulte O que é AWS Outposts? no Guia do usuário para racks do Outposts.
- Nome do grupo de segurança: o nome do grupo de segurança anexado à instância envolvida.
- ID do grupo de segurança: o ID do grupo de segurança anexado à instância envolvida.
- Estado da instância: o estado atual da instância de destino.
- Zona de disponibilidade: a zona de disponibilidade da região da AWS em que a instância envolvida está localizada.
- ID da imagem: o ID da imagem de máquina da Amazon usada para criar a instância envolvida na atividade.
- Descrição da imagem: uma descrição do ID da imagem de máquina da Amazon usada para criar a instância envolvida na atividade.
- Tags: uma lista de tags anexadas a este recurso, listadas no formato de `key:value`.

AccessKey

Detalhes da chave de acesso:

- ID da chave de acesso — A ID da chave de acesso do usuário envolvido na atividade que solicitou GuardDuty a geração da descoberta.
- ID principal — A ID principal do usuário envolvido na atividade que levou GuardDuty à geração da descoberta.
- Tipo de usuário — O tipo de usuário envolvido na atividade que levou GuardDuty à geração da descoberta. Para obter mais informações, consulte Elemento userIdentity do CloudTrail .
- Nome de usuário — O nome do usuário envolvido na atividade que levou GuardDuty à geração da descoberta.

S3Bucket

Detalhes do bucket Amazon S3:

- Nome: o nome do bucket envolvido na descoberta.
- ARN: o ARN do bucket envolvido na descoberta.
- Proprietário: o ID de usuário canônico do usuário que possui o bucket envolvido na descoberta. Para obter mais informações sobre IDs de usuário canônicos, consulte Identificadores de conta da AWS.
- Tipo: o tipo de descoberta do bucket, pode ser Destino ou Origem.
- Criptografia padrão do lado do servidor: os detalhes de criptografia para o bucket.
- Tags de bucket: uma lista de tags anexadas a esse recurso, listadas no formato de `key:value`.
- Permissões efetivas: uma avaliação de todas as permissões e políticas efetivas no bucket que indica se o bucket envolvido está exposto publicamente. Os valores podem ser públicos ou não públicos.

S3Object

- Detalhes do objeto do S3 — Inclui as seguintes informações sobre o objeto do S3:
  - ARN — Nome do recurso da Amazon (ARN) do objeto do S3 escaneado.
  - Chave - O nome atribuído ao arquivo quando ele foi criado no bucket S3.
  - ID da versão — Quando o controle de versão do bucket estiver ativado, esse campo indicará o ID da versão associado à versão mais recente do objeto do S3 verificado. Para obter mais informações, consulte Usar o versionamento em buckets do Amazon S3 no Guia do usuário do Amazon S3.

  - ETag — Representa a versão específica do objeto do S3 verificado.
  - Hash — Hash da ameaça detectada nesta descoberta.
- Detalhes do bucket do S3 — Inclui as seguintes informações sobre o bucket do Amazon S3 associado ao objeto do S3 verificado:
  - Nome - Indica o nome do bucket do S3 que contém o objeto.
  - ARN - Nome de recurso da Amazon (ARN) do bucket do S3.
- Proprietário - O ID de usuário canônico do proprietário do bucket do S3.

EKSCluster

Detalhes do cluster do Kubernetes:

- Nome: o nome do cluster do Kubernetes.
- ARN: o ARN que identifica o cluster.
- Criado em: a data e a hora em que o cluster foi criado.

> **Note**
>
> Os carimbos de data e hora das descobertas no GuardDuty console aparecem em seu fuso horário local, enquanto as exportações JSON e as saídas de CLI exibem carimbos de data e hora em UTC.

- VPC ID: o ID da VPC associada ao cluster.
- Status: o status atual do cluster.
- Tags: os metadados que você aplica ao cluster para ajudar na categorização e organização. Cada tag consiste em uma chave e um valor opcional, listados no formato `key:value`. Você pode definir a chave e o valor.

  As tags de cluster não são propagadas para nenhum outro recurso associado ao cluster.

Detalhes da workload do Kubernetes:

- Tipo: o tipo de workload do Kubernetes, como pod, implantação e trabalho.
- Nome: o nome da workload do Kubernetes.
- Uid: o ID exclusivo da workload do Kubernetes.

- Criada em: a data e a hora em que essa workload foi criada.
- Rótulos: os pares de chave-valor anexados à workload do Kubernetes.
- Contêineres: os detalhes do contêiner em execução como parte da workload do Kubernetes.
- Namespace: a workload pertence a esse namespace do Kubernetes.
- Volumes: os volumes usados pela workload do Kubernetes.
  - Caminho do host: representa um arquivo ou diretório preexistente na máquina host para a qual o volume é mapeado.
  - Nome: o nome do volume.
- contexto de segurança do pod: define as configurações de privilégio e controle de acesso para todos os contêineres em um pod.
- Rede de host: defina como `true` se os pods estão incluídos na workload do Kubernetes.

Detalhes do usuário do Kubernetes:

- Grupos: grupos com RBAC (controle baseado em acesso por função) do Kubernetes do usuário envolvido na atividade que gerou a descoberta.
- ID: ID exclusiva do usuário do Kubernetes.
- Nome de usuário: nome do usuário do Kubernetes envolvido na atividade que gerou a descoberta.
- Nome da sessão: entidade que assumiu o perfil do IAM com permissões RBAC do Kubernetes.

ECSCluster

Detalhes do cluster do ECS:

- ARN: o ARN que identifica o cluster.
- Nome: o nome do cluster.
- Status: o status atual do cluster.
- Contagem de serviços ativas: o número de serviços que estão sendo executados no cluster em um estado `ACTIVE`. Você pode ver esses serviços com ListServices
- Contagem de instâncias de contêiner registradas: o número de instâncias de contêiner registradas no cluster. Isso inclui instâncias de contêiner nos status `ACTIVE` e `DRAINING`.
- Contagem de tarefas em execução: o número de tarefas no cluster que estão no estado `RUNNING`.

- Tags: os metadados que você aplica ao cluster para ajudar na categorização e organização. Cada tag consiste em uma chave e um valor opcional, listados no formato `key:value`. Você pode definir a chave e o valor.
- Contêineres: os detalhes sobre o contêiner associado à tarefa:
  - Nome do contêiner: o nome do contêiner.
  - Imagem do contêiner: a imagem do contêiner.
- Detalhes da tarefa: os detalhes de uma tarefa em um cluster.
  - ARN: o nome do recurso da Amazon (ARN) da tarefa.
  - ARN da definição: o nome do recurso da Amazon (ARN) da definição de tarefa que cria a tarefa.
  - Versão: o contador de versões da tarefa.
  - Tarefa criada em: a data e hora do Unix quando a tarefa foi criada.
  - Tarefa iniciada em: a data e hora do Unix quando a tarefa foi iniciada.
  - Tarefa iniciada por: a tag especificada quando uma tarefa é iniciada.

Container

Detalhes do contêiner:

- Runtime do contêiner: o runtime do contêiner (como `docker` ou `containerd`) usado para executar o contêiner.
- ID: o ID da instância de contêiner ou as entradas completas do ARN para a instância de contêiner.
- Nome: o nome do contêiner.
- Imagem: a imagem da instância de contêiner.
- Montagens de volume: lista de montagens de volume de contêineres. Um contêiner pode montar um volume em seu sistema de arquivos.
- Contexto de segurança: o contexto de segurança do contêiner define as configurações de privilégio e controle de acesso para um contêiner.
- Detalhes do processo: descreve os detalhes do processo associado à descoberta.

RDSDBInstance

Detalhes da instância do RDSDB:

> **Note**
>
> Esse recurso está disponível nas descobertas da Proteção do RDS relacionadas à instância do banco de dados.

- ID da instância do banco de dados — O identificador associado à instância do banco de dados envolvida na GuardDuty descoberta.
- Mecanismo: o nome do mecanismo de banco de dados da instância do banco de dados envolvida na descoberta. Os valores possíveis são Aurora ou MySQL-Compatible Aurora. PostgreSQL-Compatible
- Versão do mecanismo — A versão do mecanismo de banco de dados envolvida na GuardDuty descoberta.
- ID do cluster do banco de dados — O identificador do cluster do banco de dados que contém o ID da instância do banco de dados envolvido na GuardDuty descoberta.
- ARN da instância do banco de dados — O ARN que identifica a instância do banco de dados envolvida na descoberta. GuardDuty

RDSLimitlessDB

Detalhes do RDSLimitlessDB:

Esse recurso está disponível nas descobertas da Proteção do RDS relacionadas à versão do mecanismo compatível do Limitless Database.

- Identificador do grupo de fragmentos de banco de dados – o nome associado ao grupo de fragmentos do Limitless DB.
- ID do recurso do grupo de fragmentos de banco de dados – o identificador do recurso do grupo de fragmentos de banco de dados dentro do Limitless DB.
- ARN do grupo de fragmentos do banco de dados – o nome do recurso da Amazon (ARN) que identifica o grupo de fragmentos do banco de dados.
- Mecanismo – o identificador do Limitless DB envolvido na descoberta.
- Versão do mecanismo – a versão do mecanismo do Limitless DB.
- Identificador de cluster de banco de dados – o nome do cluster de banco de dados que faz parte do Limitless DB.

Para obter informações sobre o usuário e detalhes da autenticação do banco de dados potencialmente afetado, consulte Detalhes do usuário do banco de dados (DB) do RDS.

Lambda

Detalhes da função do Lambda

- Nome da função: o nome da função do Lambda que está envolvida na descoberta.
- Versão da função: a versão da função do Lambda envolvida na descoberta.
- Descrição da função: uma descrição da função do Lambda envolvida na descoberta.
- ARN da função: o nome do recurso da Amazon (ARN) da função do Lambda envolvida na descoberta.
- ID da revisão: o ID da revisão da versão da função do Lambda.
- Perfil: o perfil de execução da função do Lambda envolvida na descoberta.
- Configuração da VPC: a configuração da Amazon VPC, incluindo o ID da VPC, o grupo de segurança e as IDs de sub-rede associadas à sua função do Lambda.
  - ID da VPC: o ID da Amazon VPC associado à função do Lambda envolvida na descoberta.
  - IDs de sub-rede: o ID das sub-redes associadas à sua função do Lambda.
  - Grupo de segurança: o grupo de segurança vinculado à função do Lambda envolvida. Inclui o nome do grupo de segurança e o ID do grupo.
- Tags: uma lista de tags anexadas a este recurso, listadas no formato de par de `key:value`.

Detalhes da descoberta da sequência de ataques

GuardDuty fornece detalhes de cada descoberta que ela gera em sua conta. Esses detalhes ajudam você a entender os motivos por trás da descoberta. Esta seção se concentra nos detalhes associados a Tipos de descoberta de sequência de ataque. Isso inclui insights como recursos potencialmente afetados, cronograma de eventos, indicadores, sinais e endpoints envolvidos na descoberta.

Para ver os detalhes associados aos sinais que são GuardDuty descobertas, consulte as seções associadas nesta página.

No GuardDuty console, quando você seleciona uma descoberta de sequência de ataque, o painel lateral de detalhes é dividido nas seguintes guias:

- Visão geral – fornece uma visão compacta dos detalhes da sequência de ataque, incluindo sinais, táticas do MITRE e recursos potencialmente afetados.
- Sinais – exibe uma linha do tempo dos eventos envolvidos em uma sequência de ataque.
- Recursos – fornece informações sobre os recursos potencialmente afetados ou os recursos que estão potencialmente em risco.

A lista a seguir fornece descrições associadas aos detalhes da descoberta da sequência de ataque.

Sinais

Um sinal pode ser uma atividade de API ou uma descoberta GuardDuty usada para detectar uma descoberta de sequência de ataque. GuardDuty considera os sinais fracos que não se apresentam como uma ameaça clara, os reúne e se correlaciona com as descobertas geradas individualmente. Para mais contexto, a guia Sinais fornece uma linha do tempo dos sinais, conforme observado por GuardDuty.

Cada sinal, que é uma GuardDuty descoberta, tem seu próprio nível de gravidade e valor atribuído a ele. No GuardDuty console, você pode selecionar cada sinal para ver os detalhes associados.

Atores

Fornece detalhes sobre os agentes da ameaça em uma sequência de ataque. Para obter mais informações, consulte Actor in Amazon GuardDuty API Reference.

Endpoints

Fornece detalhes sobre os endpoints de rede que foram usados nessa sequência de ataque. Para obter mais informações, consulte NetworkEndpointa Amazon GuardDuty API Reference. Para obter informações sobre como GuardDuty determina a localização, consulteDetalhes de geolocalização.

Indicadores

Inclui dados observados que correspondem ao padrão de um problema de segurança. Esses dados especificam por que GuardDuty há uma indicação de uma atividade potencialmente suspeita. Por exemplo, quando o nome do indicador é`HIGH_RISK_API`, isso indica uma ação comumente usada por agentes de ameaças ou uma ação confidencial que pode causar um impacto potencial a uma Conta da AWS, como acessar credenciais ou modificar um recurso.

A tabela a seguir inclui uma lista de indicadores potenciais e suas descrições:

Nome do indicador	Description
`ATTACK_TACTIC`	As táticas MITRE usadas pelo agente da ameaça em uma sequência de ataque. Os exemplos incluem Discovery e Impact.
`ATTACK_TECHNIQUE`	A técnica MITRE usada pelo agente da ameaça em uma sequência de ataque. Os exemplos incluem obter acesso a recursos e usá-los de forma não intencional e explorar vulnerabilidades.
`CRYPTOMINING_DOMAIN`	Indica um nome de domínio associado a infraestrutura ou pools de mineração de criptomoedas. Por exemplo, consultas ao DNS ou conexões a esses domínios a partir de ambientes de contêiner ou Kubernetes podem indicar atividade de criptomineração não autorizada.
`CRYPTOMINING_IP`	Indica um endereço IP associado a infraestrutura ou pools de mineração de criptomoedas. Por exemplo, consultas a esses endereços a partir de ambientes de contêiner ou Kubernetes podem indicar atividade de criptomineração não autorizada.
`CRYPTOMINING_PROCESS`	Indica um processo identificado como software de mineração de criptomoedas executado em ambientes de contêiner ou Kubernetes. Por exemplo, esses processos podem consumir recursos excessivos da CPU.
`HIGH_RISK_API`	A AWS API que inclui o AWS service (Serviço da AWS) nome e `eventName` indica uma ação comumente usada por agentes de ameaças ou é uma ação confidencial que pode causar um impacto potencial a uma Conta da AWS, como acesso a credenciais ou modificação de recursos.
`MALICIOUS_DOMAIN`	Indica um nome de domínio com inteligência de ameaças suspeitas indicando intenção maliciosa. Por exemplo, isso inclui servidores de comando e controle (C&C), sites de distribuição de malware ou domínios de phishing contatados a partir de ambientes de contêiner ou Kubernetes.

Nome do indicador	Description
MALICIOUS_FILE	Indica um arquivo suspeito de ser malicioso com base na inteligência de ameaças ou na análise comportamental. Por exemplo, isso inclui binários de malware conhecidos, scripts maliciosos ou executáveis não autorizados.
MALICIOUS_IP	O endereço IP confirmou a inteligência de ameaças, indicando intenção maliciosa.
MALICIOUS_PACKAGE	Indica que um recurso envolvido na sequência de ataque contém um pacote de software identificado como malicioso. Os valores do indicador incluem identificadores de pacotes maliciosos usando a designação OSV (MAL-*) associada aos pacotes detectados.
MALICIOUS_PROCESS	Indica um processo com suspeita de ser malicioso com base na inteligência de ameaças ou na análise comportamental. Por exemplo, isso inclui malware conhecido, backdoors ou ferramentas não autorizadas executadas em uma instância ou ambiente de contêiner.
MISCONFIGURATION	Indica que um recurso envolvido na sequência de ataque tem uma configuração incorreta de segurança que pode aumentar o impacto potencial. Os exemplos incluem políticas de acesso administrativo, controle de versão desativado ou criptografia ausente. Essas configurações incorretas são identificadas por. AWS Security Hub CSPM Para obter mais informações, consulte Tipos de características compatíveis no Guia AWS Security Hub CSPM do usuário.
REACHABILITY	Indica que um recurso envolvido na sequência de ataque pode ser acessado pela Internet ou acessível ao público. Os exemplos incluem instâncias do Amazon EC2 acessíveis pela Internet, clusters do Amazon EKS, clusters do Amazon ECS ou buckets do Amazon S3 acessíveis ao público. Para obter mais informações, consulte Tipos de características compatíveis no Guia AWS Security Hub CSPM do usuário.

Nome do indicador	Description
SENSITIVE_DATA	Indica que um bucket do Amazon S3 envolvido na sequência de ataque contém dados confidenciais, conforme identificados pelo Amazon Macie por meio de. AWS Security Hub CSPM
SUSPICIOUS_NETWORK	A rede está associada a pontuações conhecidas de baixa reputação, como provedores de rede privada virtual (VPN) arriscados e serviços de proxy.
SUSPICIOUS_PROCESS	Indica um processo suspeito identificado como anômalo com base na inteligência de ameaças ou na análise comportamental. Por exemplo, isso inclui padrões incomuns de execução de processos, relacionamentos pai-filho inesperados ou processos com características suspeitas em uma instância ou ambiente de contêiner.
SUSPICIOUS_USER_AGENT	O agente do usuário está associado a aplicações potencialmente conhecidas suspeitas ou exploradas, como clientes Amazon S3 e ferramentas de ataque.
TOR_IP	O endereço IP está associado a um nó de saída do Tor.
UNUSUAL_API_FOR_ACCOUNT	Indica que a AWS API foi invocada de forma anômala, com base na linha de base histórica da conta. Para obter mais informações, consulte Comportamento anômalo.
UNUSUAL_ASN_FOR_ACCOUNT	Indica que o número de sistema autônomo (ASN) foi identificado como anômalo, com base na linha de base histórica da conta. Para obter mais informações, consulte Comportamento anômalo.
UNUSUAL_ASN_FOR_USER	Indica que o número de sistema autônomo (ASN) foi identificado como anômalo, com base na linha de base histórica do usuário. Para obter mais informações, consulte Comportamento anômalo.

Nome do indicador	Description
VULNERABILITY	Indica que um recurso envolvido na sequência de ataque tem vulnerabilidades conhecidas com severidade crítica, alta, média ou baixa. Os valores do indicador incluem identificadores CVE e seus níveis de severidade. Essas vulnerabilidades são detectadas pelo Amazon Inspector e podem aumentar o impacto potencial da sequência de ataque. Para obter mais informações sobre os níveis de severidade, consulte Entendendo os níveis de gravidade no Guia do usuário do Amazon Inspector.

Táticas MITRE

Esse campo especifica as táticas do MITRE ATT&CK que o agente da ameaça tenta por meio de uma sequência de ataque. GuardDuty usa a estrutura MITRE ATT&ACK que adiciona contexto a toda a sequência de ataque. As cores que o GuardDuty console usa para especificar as finalidades da ameaça que foram usadas pelo agente da ameaça se alinham às cores que indicam a crítica, a alta, a média e a baixaNíveis de gravidade das descobertas.

Indicadores de rede

Os indicadores incluem uma combinação de valores de indicadores de rede que explicam por que uma rede é indicativa de comportamento suspeito. Esta seção é aplicável somente quando o Indicador inclui `SUSPICIOUS_NETWORK` ou`MALICIOUS_IP`. O exemplo a seguir mostra como os indicadores de rede podem ser associados a um indicador, onde:

- *AnyCompany*é um Sistema Autônomo (AS).
- `TUNNEL_VPN`, `IS_ANONYMOUS` e `ALLOWS_FREE_ACCESS` são os indicadores da rede.

```
...{
    "key": "SUSPICIOUS_NETWORK",
    "values": [{
        "AnyCompany": [
            "TUNNEL_VPN",
            "IS_ANONYMOUS",
            "ALLOWS_FREE_ACCESS"
        ]
    }]
}
...
```

A tabela a seguir inclui os valores dos indicadores de rede e sua descrição. Essas tags são adicionadas com base na inteligência de ameaças GuardDuty coletada de fontes como o Spur.

Valor do indicador de rede	Description
`TUNNEL_VPN`	A rede ou o endereço IP está associado a um tipo de túnel VPN. Isso se refere a um protocolo específico que ajuda a estabelecer uma conexão segura e criptografada entre dois pontos em uma rede pública.
`TUNNEL_PROXY`	A rede ou o endereço IP está associado a um tipo de túnel proxy. Isso se refere a um protocolo específico que ajuda a estabelecer uma conexão por meio de um servidor proxy.
`TUNNEL_RDP`	A rede ou o endereço IP está associado ao uso de um método de encapsulamento do tráfego de desktop remoto (RDP) em outro protocolo para aumentar a segurança, contornar as restrições da rede ou permitir o acesso remoto por meio de firewalls.
`IS_ANONYMOUS`	A rede ou o endereço IP está associado a serviços anônimos ou de proxy conhecidos. Isso pode indicar possíveis atividades suspeitas escondidas atrás de redes anônimas.
`KNOWN_THR EAT_OPERATOR`	A rede ou o endereço IP está associado a um tipo de túnel arriscado conhecido. Isso indica que atividades suspeitas foram detectadas a partir de um endereço IP vinculado a uma VPN, proxy ou a outros serviços de tunelamento frequentemente usados para fins maliciosos.
`ALLOWS_FR EE_ACCESS`	A rede ou o endereço IP está associado a um operador de túnel que permite o acesso ao serviço sem exigir autenticação ou pagamento. Também pode incluir contas de teste ou experiências de uso limitadas oferecidas por vários serviços on-line.
`ALLOWS_CRYPTO`	A rede ou o endereço IP está associado a um provedor de túneis (como VPN ou serviço de proxy) que aceita exclusivamente criptomoe das ou outras moedas digitais como forma de pagamento.

Valor do indicador de rede	Description
ALLOWS_TORRENTS	A rede ou o endereço IP está associado a serviços ou plataformas que permitem o tráfego de torrents. Esses serviços são frequentemente associados ao suporte e uso de torrents e atividades de evasão de direitos autorais.
RISK_CALLBACK_PROXY	A rede ou o endereço IP está associado a dispositivos conhecidos por rotear o tráfego para proxies residenciais, proxies de malware ou outras redes do tipo proxy de retorno de chamada. Isso não significa que todas as atividades na rede estejam relacionadas ao proxy, mas sim que a rede tem a capacidade de rotear o tráfego em nome dessas redes proxy.
RISK_GEO_MISMATCH	Esse indicador sugere que o datacenter ou o local de hospedagem de uma rede difere da localização esperada dos usuários e dispositivos por trás dela. Se esse valor do indicador não estiver presente, isso não significa que não há incompatibilidade. Isso pode implicar que não há dados suficientes para confirmar a discrepância.
IS_SCANNER	A rede ou o endereço IP está associado à realização de tentativas persistentes de login em formulários da web.
RISK_WEB_SCRAPING	A rede ou o endereço IP está associado a clientes web automatizados e outras atividades programáticas da web.
CLIENT_BEHAVIOR_FILE_SHARING	A rede ou o endereço IP está associado ao comportamento do cliente, indicativo de atividades de compartilhamento de arquivos, como redes ponto a ponto (P2P) ou protocolos de compartilhamento de arquivos.
CATEGORY_COMMERCIAL_VPN	A rede ou o endereço IP está associado a um operador de túnel que é classificado como um serviço tradicional de rede privada virtual (VPN) comercial operando dentro do espaço do datacenter.
CATEGORY_FREE_VPN	A rede ou o endereço IP está associado a um operador de túnel que é classificado como um serviço de VPN totalmente gratuito.

Valor do indicador de rede	Description
`CATEGORY_RESIDENTIAL_PROXY`	A rede ou o endereço IP está associado a um operador de túnel que é classificado como SDK, malware ou serviço de proxy de origem paga.
`OPERATOR_XXX`	O nome do provedor de serviços que está operando esse túnel.

Regras de detecção personalizadas encontrando detalhes

Os detalhes em uma descoberta de Regras de Detecção Personalizadas dependem da fonte de dados da regra que a gerou.

Descobertas de AWS CloudTrail regras

As descobertas das AWS CloudTrail regras usam a mesma `Service.Detection.Sequence` estrutura deDetalhes da descoberta da sequência de ataques. Os campos Atores, Pontos Finais, Recursos e Sinais compartilham o mesmo esquema. Os detalhes a seguir são específicos das Regras de Detecção Personalizadas.

Tipo

O tipo de descoberta segue o formato`Tactic:Service/Technique`. Por exemplo, .`Persistence:EC2/ExternalRemoteServices`

Sinais

Cada sinal representa um único evento de regra correspondente. O `Name` campo contém o nome das Regras de Detecção Personalizadas e `SignalIndicators` contém a tática e a técnica MITRE ATT&CK®. Vários sinais com a mesma regra podem aparecer quando a regra corresponde a vários eventos na janela de agregação.

Atores

Detalhes sobre os diretores do IAM que realizaram a atividade detectada. Inclui o tipo de usuário (como `AssumedRole` ou`IAMUser`), informações de credenciais e detalhes da sessão, incluindo o ARN da função emissora e o status do MFA.

Recursos

Detalhes sobre os AWS recursos envolvidos na atividade detectada, quando aplicável, como instâncias do Amazon EC2, buckets do Amazon S3 ou chaves de acesso do IAM.

Endpoints

Detalhes sobre os endpoints de rede dos quais a atividade se originou. Inclui o endereço IP, a localização geográfica (cidade e país) e o nome e número do sistema autônomo (AS).

Conclusões das regras de monitoramento de tempo de execução

As descobertas das regras do Runtime Monitoring usam a mesma estrutura de outras descobertas do Runtime Monitoring, incluindo os detalhes do tempo de execução do processo envolvido. Para obter mais informações, consulte Detalhes da descoberta do monitoramento de runtime. Os detalhes a seguir são específicos das Regras de Detecção Personalizadas:

Tipo

O tipo de descoberta segue o formato`Tactic:Runtime/Technique`. Por exemplo, .`Persistence:Runtime/SuspiciousCommand`

Regra

O `CustomDetectionRuleName` campo contém o nome da regra de detecção personalizada que gerou a descoberta.

Contexto

Os `Service.RuntimeDetails.Context` campos descrevem a atividade correspondente. Os campos que uma descoberta inclui dependem da regra:

- As regras que geram `SensitiveFileRead` e `SensitiveFileModified` as descobertas incluem `FilePath` `FileOperation` e.
- A maioria das regras que geram `SuspiciousCommand` descobertas incluem`CommandLineExample`, e algumas também incluem`ServiceName`. As regras que detectam atividades em um arquivo específico, como alterar as permissões do arquivo, incluem, `FilePath` em vez disso, e `FileOperation` quando se aplica.
- As regras que geram `SuspiciousTool` descobertas incluem `ToolName` `ToolCategory` e.

Recurso

Cada descoberta abrange um único recurso, como uma instância, uma tarefa ou um contêiner. Para obter mais informações sobre como os GuardDuty grupos sinalizam, consulteEncontrando agregação.

Detalhes do usuário do banco de dados (DB) do RDS

> **Note**
>
> Esta seção é aplicável às descobertas quando você ativa o recurso de Proteção do RDS no GuardDuty. Para obter mais informações, consulte GuardDuty Proteção RDS.

A GuardDuty descoberta fornece os seguintes detalhes de usuário e autenticação do banco de dados potencialmente comprometido:

- Usuário: o nome de usuário usado para fazer a tentativa anômala de login.
- Aplicação: o nome da aplicação usada para fazer a tentativa anômala de login.
- Banco de dados: o nome da instância do banco de dados envolvida na tentativa anômala de login.
- SSL: a versão do Secure Socket Layer (SSL) usada para a rede.
- Método de autenticação: o método de autenticação usado pelo usuário envolvido na descoberta.

Para obter informações sobre o recurso potencialmente comprometido, consulte Recurso.

Detalhes da descoberta do monitoramento de runtime

> **Note**
>
> Esses detalhes podem estar disponíveis somente se GuardDuty gerar um dosGuardDuty Tipos de descoberta de monitoramento de tempo de execução.

Esta seção contém os detalhes do runtime, como detalhes do processo e qualquer contexto necessário. Os detalhes do processo descrevem as informações sobre o processo observado e o contexto do runtime descreve qualquer informação adicional sobre a atividade potencialmente suspeita.

Detalhes do processo

- Nome: o nome do processo.
- Caminho do executável: o caminho absoluto do arquivo executável do processo.
- Executável SHA-256 — O `SHA256` hash do executável do processo.
- PID do Namespace: o ID do processo em um namespace PID secundário diferente do namespace PID no nível do host. Para processos em um contêiner, é o ID do processo observado dentro do contêiner.
- Diretório de trabalho atual: o diretório de trabalho atual do processo.
- ID do processo: o ID atribuído ao processo pelo sistema operacional.
- startTime: a hora em que o processo foi iniciado. Está no formato de string de data UTC (`2023-03-22T19:37:20.168Z`).
- UUID — O ID exclusivo atribuído ao processo por. GuardDuty
- UUID principal: o ID exclusivo do processo principal. Essa ID é atribuída ao processo principal por GuardDuty.
- Usuário: o usuário que executou o processo.
- ID do usuário: o ID do usuário que executou o processo.
- ID de usuário efetivo: o ID de usuário efetivo do processo no momento do evento.
- Linhagem: informações sobre os ancestrais do processo.
  - ID do processo: o ID atribuído ao processo pelo sistema operacional.
  - UUID — O ID exclusivo atribuído ao processo por. GuardDuty
  - Caminho do executável: o caminho absoluto do arquivo executável do processo.
  - ID de usuário efetivo: o ID de usuário efetivo do processo no momento do evento.
  - UUID principal: o ID exclusivo do processo principal. Essa ID é atribuída ao processo principal por GuardDuty.
  - Hora de início: o hora em que o processo foi iniciado.
  - PID do Namespace: o ID do processo em um namespace PID secundário diferente do namespace PID no nível do host. Para processos em um contêiner, é o ID do processo observado dentro do contêiner.
  - ID do usuário: o ID do usuário que executou o processo.
  - Nome: o nome do processo.

Contexto de runtime

Com os campos a seguir, uma descoberta gerada pode incluir somente os campos relevantes para o tipo de descoberta.

- Origem de montagem: o caminho no host que é montado pelo contêiner.
- Destino de montagem: o caminho no contêiner que é mapeado para o diretório do host.
- Tipo de sistema de arquivos: representa o tipo do sistema de arquivos montado.
- Sinalizadores: representam opções que controlam o comportamento do evento envolvido nessa descoberta.
- Processo de modificação: informações sobre o processo que criou ou modificou um binário, script ou biblioteca dentro de um contêiner no runtime.
- Modificado em: o carimbo de data/hora em que o processo criou ou modificou um binário, script ou biblioteca dentro de um contêiner no runtime. Esse campo está no formato de string de data UTC (`2023-03-22T19:37:20.168Z`).
- Caminho da biblioteca: o caminho para a nova biblioteca que foi carregada.
- Valor de LD Preload: o valor da variável de ambiente `LD_PRELOAD`.
- Caminho do soquete: o caminho para o soquete do Docker que foi acessado.
- Caminho do binário Runc: o caminho para o binário `runc`.
- Caminho do agente de liberação: o caminho para o arquivo do agente de liberação `cgroup`.
- Exemplo de linha de comando — O exemplo da linha de comando envolvida na possível atividade suspeita.
- Categoria da ferramenta — Categoria à qual a ferramenta pertence. Alguns dos exemplos são Backdoor Tool, Pentest Tool, Network Scanner e Network Sniffer.
- Nome da ferramenta — O nome da ferramenta possivelmente suspeita.
- Operação de arquivo — O tipo de operação de arquivo que acionou a descoberta, como gravar, excluir, renomear, vincular ou link simbólico.
- Caminho do arquivo — O caminho do arquivo confidencial que foi modificado. A modificação inclui operações de gravação, exclusão, renomeação, vinculação ou link simbólico.
- Caminhos de arquivo relacionados — Todos os caminhos de arquivo foram modificados pelo mesmo processo que acionou a descoberta, até um máximo de 25 caminhos.
- Caminho do script — O caminho para o script executado que gerou a descoberta.
- Caminho do arquivo da ameaça — O caminho suspeito cujos detalhes de inteligência contra ameaças foram encontrados.

- Nome do serviço — O nome do serviço de segurança que foi desabilitado.
- Nome do módulo – o nome do módulo carregado no kernel.
- Módulo SHA256 – o hash SHA256 do módulo.
- Caminho do arquivo do módulo – o caminho para o módulo carregado no kernel.

Detalhes de verificação de volumes do EBS

> **Note**
>
> Esta seção é aplicável às descobertas quando você ativa a verificação de GuardDuty-initiated malwareProteção contra malware para o EC2.

A análise de volumes do EBS fornece detalhes sobre o volume do EBS anexado à instância EC2 ou à workload do contêiner potencialmente comprometida.

- ID da verificação: o identificador da verificação de malware.
- Verificação começou em: a data e a hora em que a verificação de malware foi iniciado.
- Verificação concluída em: a data e hora em que foi concluída a verificação de malware.
- Trigger Finding ID — O ID de GuardDuty descoberta da descoberta que iniciou essa verificação de malware.
- Fontes — Os valores potenciais são `Bitdefender` e `Amazon`.

  Para obter mais informações sobre o mecanismo de verificação usado para detectar malware, consulte GuardDuty mecanismo de verificação de detecção de malware.
- Detecções de verificações: a visão completa dos detalhes e resultados de cada verificação de malware.
  - Contagem de itens verificados: o número total de arquivos verificados. Fornece detalhes como `totalGb`, `files` e `volumes`.
  - Contagem de itens detectados por ameaças: o número total de `files` mal-intencionados detectados durante a verificação.
  - Detalhes da ameaça de maior gravidade: os detalhes da ameaça de maior gravidade detectada durante a verificação e o número de arquivos mal-intencionados. Fornece detalhes como `severity`, `threatName` e `count`.

- Ameaças detectadas por nome: o elemento de contêiner que agrupa ameaças de todos os níveis de gravidade. Fornece detalhes como `itemCount`, `uniqueThreatNameCount`,`shortened` e `threatNames`.

Detalhes de descobertas sobre a Proteção contra malware para EC2

> **Note**
>
> Esta seção é aplicável às descobertas quando você ativa a verificação de GuardDuty-initiated malwareProteção contra malware para o EC2.

Quando o escaneamento do Malware Protection for EC2 detecta malware, você pode visualizar os detalhes do escaneamento selecionando a descoberta correspondente na página Descobertas no https://console.aws.amazon.com/guardduty/console. A gravidade da descoberta do Malware Protection for EC2 depende da gravidade da GuardDuty descoberta.

As informações exibidas a seguir estão disponíveis na seção Ameaças detectadas no painel de detalhes.

- Nome: o nome da ameaça, obtido ao agrupar os arquivos por detecção.
- Gravidade: a gravidade da ameaça detectada.
- Hash — O SHA-256 do arquivo.
- Caminho do arquivo: a localização do arquivo mal-intencionado no volume do EBS.
- Nome do arquivo: o nome do arquivo em que a ameaça foi detectada.
- ARN do volume: o ARN dos volumes do EBS verificados.

As informações a seguir estão disponíveis na seção Detalhes do verificação de malware no painel de detalhes.

- ID de verificação: o ID de verificação da verificação de malware.
- Verificação começou em: a data e a hora em que a verificação foi iniciada.
- Verificação concluída em: a data e a hora em que a verificação foi concluída.
- Arquivos verificados: o número total de arquivos e diretórios verificados.
- Total de GB verificados: a quantidade de armazenamento verificada durante o processo.

- ID de descoberta do gatilho — O ID de GuardDuty descoberta da descoberta que iniciou essa verificação de malware.
- As informações exibidas a seguir estão disponíveis na seção Detalhes do volume no painel de detalhes.
  - ARN do volume: o nome do recurso da Amazon (ARN) do volume.
  - SnapshotARN: o ARN do snapshot do volume do EBS.
  - Status: o status de verificação do volume, como`Running`, `Skipped` e `Completed`.
  - Tipo de criptografia: o tipo de criptografia usado para criptografar o volume. Por exemplo, `.CMCMK`
  - Nome do dispositivo: o nome do dispositivo. Por exemplo, `./dev/xvda`

Detalhes de descobertas sobre a Proteção contra malware para S3

Os seguintes detalhes do escaneamento de malware estão disponíveis quando você ativa o Malware Protection for S3 no seu Conta da AWS: GuardDuty

- Ameaças — Uma lista das ameaças detectadas durante a verificação do malware.

> Várias ameaças potenciais em arquivos.
>
> Se você tiver um arquivo com várias ameaças potenciais, a Proteção contra Malware para S3 reportará somente a primeira ameaça detectada. Depois disso, o status da verificação é marcado como concluído. GuardDuty gera o tipo de descoberta associado e também envia EventBridge os eventos que ele gera. Para obter mais informações sobre o monitoramento das varreduras de objetos do Amazon S3 usando os EventBridge eventos, consulte o exemplo de esquema de notificação para THREATS_FOUND em. Resultado da verificação de objetos do S3

- Caminho do item — Uma lista do caminho do item aninhado e dos detalhes de hash do objeto S3 escaneado.
  - Caminho do item aninhado — Caminho do item do objeto S3 escaneado em que a ameaça foi detectada.

    O valor desse campo só estará disponível se o objeto de nível superior for um arquivo e se a ameaça for detectada dentro de um arquivo.
  - Hash — Hash da ameaça detectada nesta descoberta.

> **Note**
>
> Nos casos em que o hash não pode ser calculado, o resultado da verificação ainda é entregue e o valor do hash é padronizado para uma string vazia (). SHA-256 `e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855`

- Fontes — Os valores potenciais são `Bitdefender` e `Amazon`.

  Para obter mais informações sobre o mecanismo de verificação usado para detectar malware, consulte GuardDuty mecanismo de verificação de detecção de malware.

Ação

A Ação de uma descoberta fornece detalhes sobre o tipo de atividade que acionou a descoberta. As informações disponíveis variam com base no tipo de ação.

Tipo de ação: o tipo de atividade de descoberta. Esse valor pode ser NETWORK_CONNECTION, PORT_PROBE, DNS_REQUEST ou RDS_LOGIN_ATTEMPT. AWS_API_CALL As informações disponíveis variam com base no tipo de ação:

- NETWORK_CONNECTION: indica que o tráfego de rede foi trocado entre a instância do EC2 identificada e o host remoto. Esse tipo de ação tem as seguintes informações adicionais:
  - Direção da conexão — A direção da conexão de rede observada na atividade que levou GuardDuty à geração da descoberta. Os valores podem ser:
    - INBOUND: indica que um host remoto iniciou uma conexão a uma porta local na instância do EC2 identificada na conta.
    - OUTBOUND: indica que a instância do EC2 identificada iniciou uma conexão a um host remoto.
    - DESCONHECIDO — Indica que não GuardDuty foi possível determinar a direção da conexão.
  - Protocolo — O protocolo de conexão de rede observado na atividade que levou GuardDuty à geração da descoberta.
  - IP local: o endereço IP de origem original do tráfego que acionou a descoberta. Essas informações podem ser usadas para fazer a distinção entre o endereço IP de uma camada intermediária pela qual o tráfego flui e o endereço IP de origem original do tráfego que acionou a descoberta. Por exemplo, o endereço IP de um pod do EKS em oposição ao endereço IP da instância em que o pod do EKS está sendo executado.

  - Bloqueado: indica se a porta de destino está bloqueada.
- PORT_PROBE: indica que um host remoto consultou a instância do EC2 identificada em várias portas abertas. Esse tipo de ação tem as seguintes informações adicionais:
  - IP local: o endereço IP de origem original do tráfego que acionou a descoberta. Essas informações podem ser usadas para fazer a distinção entre o endereço IP de uma camada intermediária pela qual o tráfego flui e o endereço IP de origem original do tráfego que acionou a descoberta. Por exemplo, o endereço IP de um pod do EKS em oposição ao endereço IP da instância em que o pod do EKS está sendo executado.
  - Bloqueado: indica se a porta de destino está bloqueada.
- DNS_REQUEST: indica que a instância do EC2 identificada consultou um nome de domínio. Esse tipo de ação tem as seguintes informações adicionais:
  - Protocolo — O protocolo de conexão de rede observado na atividade que levou GuardDuty à geração da descoberta.
  - Bloqueado: indica se a porta de destino está bloqueada.
- AWS_API_CALL— Indica que uma AWS API foi invocada. Esse tipo de ação tem as seguintes informações adicionais:
  - API — O nome da operação de API que foi invocada e, portanto, solicitada GuardDuty para gerar essa descoberta.

    > **Note**
    >
    > Essas operações também podem incluir eventos que não são de API capturados pelo AWS CloudTrail. Para obter mais informações, consulte Non-API eventos capturados por CloudTrail.

  - Agente do usuário: o agente do usuário que fez a solicitação da API. Esse valor informa se a chamada foi feita a partir do Console de gerenciamento da AWS, de um AWS serviço, dos AWS SDKs ou do AWS CLI.
  - CÓDIGO DE ERRO: se a descoberta foi acionada por uma falha na chamada de API, o código de erro dessa chamada será exibido.
  - Nome do serviço: o nome DNS do serviço que tentou fazer a chamada de API que acionou a descoberta.
- RDS_LOGIN_ATTEMPT: indica que foi feita uma tentativa de login no banco de dados potencialmente comprometido de um endereço IP remoto.

- Endereço IP: o endereço IP remoto usado para fazer a tentativa de login potencialmente suspeita.

Agente ou destino

Uma descoberta terá uma seção Agente se a Função do recurso for `TARGET`. Isso indicará que o recurso foi alvo de atividades suspeitas, e a seção Agente apresentará detalhes sobre a entidade que apontou para o recurso.

Uma descoberta terá uma seção Destino se a Função do recurso for `ACTOR`. Isso indica que o recurso estava envolvido em atividades suspeitas em um host remoto, e essa seção contém informações sobre o IP e/ou domínio para o qual o recurso apontou.

As informações disponíveis em uma seção Agente ou Destino podem incluir:

- Afiliado — Detalhes sobre se a AWS conta do chamador remoto da API está relacionada ao seu GuardDuty ambiente. Se esse valor for `true`, o chamador da API está afiliado à sua conta de alguma forma. Se for `false`, o chamador da API é de fora do seu ambiente.
- ID da conta remota: o ID da conta que possui o endereço IP de saída usado para acessar o recurso na rede final.
- Endereço IP — O endereço IP envolvido na atividade que levou GuardDuty à geração da descoberta.
- Localização — Informações de localização do endereço IP envolvido na atividade que levou GuardDuty à geração da descoberta.
- Organização — informações da organização do ISP sobre o endereço IP envolvido na atividade que levou GuardDuty à geração da descoberta.
- Porta — O número da porta envolvida na atividade que levou GuardDuty à geração da descoberta.
- Domínio — O domínio envolvido na atividade que levou GuardDuty à geração da descoberta.
- Domínio com sufixo — O domínio de segundo e primeiro nível envolvido em uma atividade que potencialmente levou GuardDuty à geração da descoberta. Para obter uma lista de domínios de primeiro e segundo nível, consulte a lista pública de sufixos.

Detalhes de geolocalização

GuardDuty determina a localização e a rede das solicitações usando bancos de dados MaxMind GeoIP. MaxMind relata uma precisão muito alta de seus dados em nível de país, embora a precisão varie de acordo com fatores como país e tipo de endereço IP.

Para obter mais informações sobre MaxMind, consulte Geolocalização MaxMind IP. Se você acredita que algum dado do GeoIP está incorreto, envie uma solicitação de correção para MaxMind MaxMindCorrigir dados do GeoIP2.

Mais informações

Todas as descobertas têm uma seção Informações adicionais que pode incluir as seguintes informações:

- Nome da lista de ameaças — O nome da lista de ameaças que inclui o endereço IP ou o nome de domínio envolvido na atividade que levou GuardDuty à geração da descoberta.
- Amostra: um valor verdadeiro ou falso que indica se é uma descoberta de amostra.
- Arquivada: um valor verdadeiro ou falso que indica se essa descoberta foi arquivada.
- Incomum: detalhes da atividade que não foram observados historicamente. Eles podem incluir um usuário, local, hora, bucket, comportamento de login ou ASN Org incomum (não observado anteriormente).
- Protocolo incomum — O protocolo de conexão de rede envolvido na atividade que levou GuardDuty à geração da descoberta.
- Detalhes do agente: detalhes sobre o agente de segurança que está atualmente implantado no cluster do EKS em sua Conta da AWS. Isso só se aplica aos tipos de descoberta do Monitoramento de runtime do EKS.
  - Versão do agente — A versão do agente GuardDuty de segurança.
  - ID do agente — O identificador exclusivo do agente GuardDuty de segurança.

Evidência

As descobertas baseadas na inteligência de ameaças têm uma seção Evidência que inclui as seguintes informações:

- Detalhes da inteligência de ameaças: o nome da lista de ameaças na qual o `Threat name` reconhecido aparece.

- Nome da ameaça: o nome da família de malware, ou outro identificador, associado à ameaça.
- Arquivo de ameaça SHA256 — SHA256 do arquivo que gerou a descoberta.

Comportamento anômalo

Os tipos de descobertas que terminam em AnomalousBehaviorindicam que a descoberta foi gerada pelo modelo de aprendizado de máquina (ML) de detecção de GuardDuty anomalias. O modelo de machine learning avalia todas as solicitações de API para sua conta e identifica eventos anômalos associados às táticas usadas pelos adversários. O modelo de machine learning rastreia vários fatores da solicitação de API, como o usuário que fez a solicitação, o local de onde a solicitação foi feita e a API específica que foi solicitada.

Detalhes sobre quais fatores da solicitação de API são incomuns para a identidade CloudTrail do usuário que invocou a solicitação podem ser encontrados nos detalhes da descoberta. As identidades são definidas pelo elemento CloudTrail UserIdentity e os valores possíveis sãoRoot:IAMUser,,, AssumedRole FederatedUserAWSAccount, ou. AWSService

Além dos detalhes disponíveis para todas as GuardDuty descobertas associadas à atividade da API, AnomalousBehavioras descobertas têm detalhes adicionais que são descritos na seção a seguir. É possível visualizar esses detalhes no console e eles também estão disponíveis no JSON da descoberta.

- APIs anômalas: uma lista de solicitações de API que foram invocadas pela identidade do usuário nas proximidades da solicitação de API primária associada à descoberta. Esse painel traz ainda mais detalhes do evento da API das maneiras a seguir.
  - A primeira API listada é a API primária, que é a solicitação de API associada à atividade de maior risco observada. Essa é a API que acionou a descoberta e se correlaciona ao estágio de ataque do tipo de descoberta. Essa também é a API detalhada na seção Ação do console e no JSON da descoberta.
  - Todas as outras APIs listadas são APIs anômalas adicionais provenientes da identidade de usuário listada observada nas proximidades da API principal. Se houver apenas uma API na lista, o modelo de machine learning não identificou nenhuma solicitação de API adicional dessa identidade de usuário como anômala.
  - A lista de APIs é dividida com base no fato de uma API ter sido chamada com êxito ou se a API foi chamada sem êxito, o que significa que uma resposta de erro foi recebida. O tipo de resposta de erro recebida está listado acima de cada API chamada sem êxito. Os possíveis tipos de resposta de erro são: `access denied`, `access denied exception`, `auth`

`failure`, `instance limit exceeded`, `invalid permission - duplicate`, `invalid permission - not found` e `operation not permitted`.

- As APIs são categorizadas pelo serviço associado a elas.
- Para mais contexto, escolha APIs históricas para visualizar os detalhes das principais APIs, até um máximo de 20, geralmente vistas tanto para a identidade do usuário quanto para todos os usuários da conta. As APIs são marcadas como Raras (menos de uma vez por mês), Infrequentes (algumas vezes por mês) ou Frequentes (diárias a semanais), dependendo da frequência em que são usadas na conta.

- Comportamento incomum (conta): esta seção fornece detalhes adicionais sobre o comportamento descrito para a conta.

> **Comportamento de perfil**
>
> GuardDuty aprende continuamente sobre as atividades em sua conta com base nos eventos entregues. Essas atividades e sua frequência observada são conhecidas como comportamento de perfil.

  As informações rastreadas nesse painel incluem:

  - ASN Org: o número de sistema autônomo (ASN) da Org da qual a chamada de API anômala foi feita.
  - Nome de usuário: o nome do usuário que fez a chamada de API anômala.
  - Agente do usuário: o agente do usuário usado para fazer a chamada de API anômala. O agente do usuário é o método usado para fazer a chamada, como `aws-cli` ou `Botocore`.
  - Tipo de usuário: o tipo de usuário que fez a chamada de API anômala. Os valores possíveis são `AWS_SERVICE`, `ASSUMED_ROLE`, `IAM_USER` ou `ROLE`.
  - Bucket: o nome do bucket do S3 que está sendo acessado.

- Comportamento incomum (identidade do usuário): esta seção fornece detalhes adicionais sobre o comportamento descrito para a identidade do usuário envolvida na descoberta. Quando um comportamento não é identificado como histórico, isso significa que o modelo de GuardDuty ML não viu anteriormente essa identidade de usuário fazendo essa chamada de API dessa forma durante o período de treinamento. Estes detalhes adicionais sobre a identidade do usuário estão disponíveis:

  - ASN Org: o ASN Org do qual a chamada de API anômala foi feita.

  - Agente do usuário: o agente do usuário usado para fazer a chamada de API anômala. O agente do usuário é o método usado para fazer a chamada, como `aws-cli` ou `Botocore`.
  - Bucket: o nome do bucket do S3 que está sendo acessado.
- Comportamento incomum (bucket): esta seção fornece detalhes adicionais sobre o comportamento perfilado do bucket do S3 associado à descoberta. Quando um comportamento não é identificado como histórico, isso significa que o modelo de GuardDuty ML não viu anteriormente chamadas de API feitas para esse bucket dessa forma durante o período de treinamento. As informações rastreadas nessa seção incluem:
  - ASN Org: o ASN Org do qual a chamada de API anômala foi feita.
  - Nome de usuário: o nome do usuário que fez a chamada de API anômala.
  - Agente do usuário: o agente do usuário usado para fazer a chamada de API anômala. O agente do usuário é o método usado para fazer a chamada, como `aws-cli` ou `Botocore`.
  - Tipo de usuário: o tipo de usuário que fez a chamada de API anômala. Os valores possíveis são `AWS_SERVICE`, `ASSUMED_ROLE`, `IAM_USER` ou `ROLE`.

  > **Note**
  >
  > Para obter mais contexto sobre comportamentos históricos, selecione Comportamento histórico na seção Comportamento incomum (conta), ID de usuário ou Bucket para ver detalhes sobre o comportamento esperado em sua conta para cada uma das seguintes categorias: Raro (menos de uma vez por mês), Infrequente (algumas vezes por mês) ou Frequente (diário ou semanal), dependendo da frequência em que são usados em sua conta.
- Comportamento incomum (banco de dados): essa seção fornece detalhes adicionais sobre o comportamento perfilado da instância do banco de dados associada à descoberta. Quando um comportamento não é identificado como histórico, isso significa que o modelo de GuardDuty ML não viu anteriormente uma tentativa de login feita nessa instância de banco de dados dessa forma durante o período de treinamento. As informações rastreadas para essa seção no painel de descoberta incluem:
  - Nome de usuário: o nome de usuário usado para fazer a tentativa anômala de login.
  - ASN Org: o ASN Org da qual a tentativa anômala de login foi feita.
  - Nome da aplicação: o nome da aplicação usada para fazer a tentativa anômala de login.
  - Nome do banco de dados: o nome da instância do banco de dados envolvida na tentativa de login anômala.

A seção Comportamento histórico fornece mais contexto sobre os nomes de usuário, ASN Orgs, nomes de aplicações e nomes de bancos de dados observados anteriormente para o banco de dados associado. Cada valor exclusivo possui uma contagem associada que representa o número de vezes que esse valor foi observado em um evento de login bem-sucedido.

- Comportamento incomum (cluster do Kubernetes da conta, namespace do Kubernetes e nome de usuário do Kubernetes): essa seção fornece mais detalhes sobre o comportamento do perfil do cluster e do namespace do Kubernetes associado à descoberta. Quando um comportamento não é identificado como histórico, isso significa que o modelo de GuardDuty ML não observou anteriormente essa conta, cluster, namespace ou nome de usuário dessa forma. As informações rastreadas para essa seção no painel de descoberta incluem:
  - Nome de usuário: o usuário que chamou a API do Kubernetes associada à descoberta.
  - Nome do usuário personificado: o usuário que está sendo personificado por `username`.
  - Namespace: o namespace do Kubernetes dentro do cluster Amazon EKS em que a ação ocorreu.
  - Agente do usuário: o agente do usuário associado à chamada de API do Kubernetes. O agente do usuário é o método usado para fazer a chamada, como `kubectl`.
  - API: a API do Kubernetes chamada pelo `username` dentro do cluster do Amazon EKS.
  - Informações de ASN: as informações de ASN, como organização e ISP, associadas ao endereço IP do usuário que está fazendo essa chamada.
  - Dia da semana: o dia da semana em que a chamada de API do Kubernetes foi feita.
  - Permissão: o verbo e o recurso do Kubernetes que estão sendo verificados quanto ao acesso para indicar se o `username` pode ou não usar a API do Kubernetes.
  - Nome da conta de serviço: a conta de serviço associada à workload do Kubernetes que fornece uma identidade à workload.
  - Registro: o registro do contêiner associado à imagem do contêiner que é implantada na workload do Kubernetes.
  - Imagem: a imagem do contêiner, sem as tags e o resumo associados, que é implantada na workload do Kubernetes.
  - Configuração de prefixo de imagem: o prefixo da imagem com o contêiner e a configuração de segurança da workload habilitados, como `hostNetwork` ou `privileged`, para o contêiner que usa a imagem.
  - Nome do assunto: os assuntos, como um `user`, `group` ou `serviceAccountName` que estão vinculados a uma função de referência em um `RoleBinding` ou `ClusterRoleBinding`.

- Nome da função: o nome da função envolvida na criação ou modificação das funções ou da API `roleBinding`.

Anomalias com base em volume do S3

Esta seção detalha as informações contextuais relacionadas a anomalias baseadas em volume do S3. A descoberta baseada em volume (Exfiltration:S3/AnomalousBehavior) monitora números incomuns de chamadas de API do S3 feitas aos buckets do S3 pelos usuários, indicando uma possível exfiltração de dados. As chamadas de API do S3 a seguir são monitoradas em relação à detecção de anomalias com base em volume.

- `GetObject`
- `CopyObject.Read`
- `SelectObjectContent`

As métricas a seguir ajudariam a criar uma linha de base do comportamento normal quando uma entidade do IAM acessa um bucket do S3. Para detectar a exfiltração de dados, a descoberta de detecção de anomalias com base em volume avalia todas as atividades em relação à linha de base comportamental usual. Selecione Comportamento histórico nas seções Comportamento incomum (identidade do usuário), Volume observado (identidade do usuário) e Volume observado (bucket) para visualizar as seguintes métricas, respectivamente.

- Número de chamadas da API `s3-api-name` invocadas pelo usuário do IAM ou pelo perfil do IAM (depende de qual deles foi emitido) associados ao bucket do S3 afetado nas últimas 24 horas.
- Número de chamadas da API `s3-api-name` invocadas pelo usuário do IAM ou pelo perfil do IAM (depende de qual deles foi emitido) associados a todos os buckets do S3 nas últimas 24 horas.
- Número de chamadas da API `s3-api-name` em todos os usuários ou perfis do IAM (depende de qual deles foi emitido) associados ao bucket do S3 afetado nas últimas 24 horas.

Anomalias baseadas na atividade de login do RDS

Esta seção detalha a contagem de tentativas de login realizadas pelo agente incomum e é agrupada pelo resultado das tentativas de login. Os Tipos de descoberta da Proteção do RDS identificam comportamentos anômalos monitorando os eventos de login em busca de padrões incomuns de `successfulLoginCount`, `failedLoginCount` e `incompleteConnectionCount`.

- successful LoginCount — Esse contador representa a soma das conexões bem-sucedidas (combinação correta de atributos de login) feitas na instância do banco de dados pelo ator incomum. Os atributos de login incluem o nome de usuário, a senha e o nome do banco de dados.
- falhou LoginCount — Esse contador representa a soma das tentativas de login falhadas (malsucedidas) feitas para estabelecer uma conexão com a instância do banco de dados. Isso indica que um ou mais atributos da combinação de login, como o nome de usuário, a senha ou o nome do banco de dados, estavam incorretos.
- incompleto ConnectionCount — Esse contador representa o número de tentativas de conexão que não podem ser classificadas como bem-sucedidas ou malsucedidas. Essas conexões são encerradas antes que o banco de dados forneça uma resposta. Por exemplo, verificação de portas em que a porta do banco de dados está conectada, mas nenhuma informação é enviada ao banco de dados, ou a conexão foi interrompida antes que o login fosse concluído em uma tentativa bem-sucedida ou malsucedida.

Anomalias baseadas em atividades de dados do RDS

Esta seção descreve atividades anômalas de dados, como um ator lendo significativamente mais linhas ou excluindo ou descartando mais dados do que o normal para esse banco de dados e usuário. Eles Tipos de descoberta da Proteção do RDS identificam comportamentos anômalos monitorando a atividade do banco de dados em busca de padrões incomuns no número de linhas lidas ou excluídas e nas instruções de descarte.

- `selectedRowse selectStatement` — Esses contadores representam o número de linhas retornadas pelas `SELECT` declarações e o número de `SELECT` declarações observadas na atividade associada à descoberta.
- `deletedRowse deleteStatement` — Esses contadores representam o número de linhas excluídas pelas `DELETE` declarações e o número de `DELETE` declarações observadas na atividade associada à descoberta.
- `dropStatement`— Esse contador representa o número de operações destrutivas, como `DROP` ou`TRUNCATE`, que podem remover objetos do banco de dados ou dados na atividade associada à descoberta.

GuardDuty pode coletar telemetria adicional de atividades de dados, como novos contadores, no futuro para melhorar a eficácia das descobertas de atividades de dados e introduzir novas detecções de ameaças do RDS Protection.

GuardDuty encontrando agregação

GuardDuty atualiza dinamicamente as descobertas geradas. Se GuardDuty detectar uma nova atividade relacionada ao mesmo problema de segurança, em vez de criar uma nova descoberta, GuardDuty atualizará a descoberta original com os detalhes mais recentes. Esse comportamento permite que os problemas em andamento sejam identificados, sem a necessidade de examinar vários relatórios semelhantes, e reduz o volume geral de descobertas para problemas de segurança conhecidos.

Por exemplo, para uma descoberta UnauthorizedAccess:EC2/SSHBruteForce, múltiplas tentativas de acesso à sua instância serão agregadas ao mesmo ID da descoberta, aumentando o número da Contagem nos detalhes da descoberta. Isso ocorre porque essa descoberta representa um único problema de segurança com a instância, indicando que a porta SSH da instância não está adequadamente protegida contra esse tipo de atividade. No entanto, se o GuardDuty detectar uma atividade de acesso SSH direcionada a uma nova instância no ambiente, ele criará uma nova descoberta com um ID de descoberta exclusivo para alertar você sobre o fato de que há um problema de segurança associado ao novo recurso.

Quando uma descoberta é agregada, ela é atualizada com as informações da última ocorrência dessa atividade. Quando uma descoberta é agregada, ela é atualizada com as informações da ocorrência mais recente dessa atividade, o que significa que, no exemplo acima, se sua instância for alvo de uma tentativa de força bruta de um novo ator, os detalhes da descoberta serão atualizados para refletir o IP remoto da fonte mais recente e as informações mais antigas serão substituídas. Informações completas sobre tentativas de atividades individuais ainda estarão disponíveis em seus CloudTrail registros ou nos registros de fluxo da VPC.

Os critérios que alertam GuardDuty para gerar uma nova descoberta em vez de agregar uma existente dependem do tipo de descoberta. Os critérios de agregação para cada tipo de descoberta são determinados por nossos engenheiros de segurança para fornecer uma visão geral de diferentes problemas de segurança na sua conta.

Quando GuardDuty gera um tipo de descoberta de sequência de ataque em sua conta, a descoberta será agregada somente quando você GuardDuty identificar os sinais semelhantes na mesma sequência em sua conta. Caso contrário, GuardDuty gerará outra sequência de ataque.

Gerenciando as GuardDuty descobertas da Amazon

GuardDuty oferece vários recursos importantes para ajudá-lo a classificar, armazenar e gerenciar suas descobertas. Esses recursos ajudarão você a adaptar as descobertas ao seu ambiente específico, reduzir o ruído de descobertas de baixo valor e ajudá-lo a se concentrar nas ameaças ao seu AWS ambiente exclusivo. Analise os tópicos desta página para entender como é possível usar esses recursos para aumentar o valor das descobertas de segurança em seu ambiente.

Tópicos:

Painel de resumo na Amazon GuardDuty

Saiba mais sobre os componentes do painel de resumo disponíveis no GuardDuty console.

Filtrando descobertas em GuardDuty

Saiba como filtrar GuardDuty as descobertas com base nos critérios que você especifica.

Regras de supressão em GuardDuty

Saiba como filtrar automaticamente as descobertas que você GuardDuty recebe por meio de regras de supressão. As regras de supressão arquivam automaticamente as descobertas com base em filtros.

Customizing threat detection with entity lists and IP address lists

Personalize o escopo do GuardDuty monitoramento usando listas de IP e listas de ameaças com base em endereços IP roteáveis publicamente. As listas de IP confiáveis evitam que descobertas não DNS sejam geradas a partir de IPs que você considera confiáveis, enquanto as listas Threat Intel farão GuardDuty com que você alerte sobre atividades de IPs definidos pelo usuário.

Exportar as descobertas geradas para bucket do Amazon S3

Exporte as descobertas geradas para um bucket do Amazon S3 para que você possa manter registros após o período de retenção das descobertas de 90 dias em. GuardDuty Use esses dados históricos para rastrear possíveis atividades suspeitas em sua conta e avaliar se as etapas de correção recomendadas foram executadas com sucesso.

Processando GuardDuty descobertas com a Amazon EventBridge

Configure notificações automáticas para GuardDuty descobertas por meio de EventBridge eventos da Amazon. Você também pode automatizar outras tarefas EventBridge para ajudá-lo a responder às descobertas.

Entendendo CloudWatch os registros e os motivos para pular recursos durante a verificação do Malware Protection for EC2

Saiba como você pode auditar os CloudWatch registros de proteção contra GuardDuty malware do EC2 e quais são os motivos pelos quais sua instância do Amazon EC2 ou volumes do Amazon EBS afetados podem ter sido ignorados durante o processo de verificação.

Denunciando falsos positivos na Proteção contra malware para EC2

Saiba como você pode denunciar possíveis detecções de ameaças de falsos positivos no Malware Protection for EC2.

Relatar o resultado da verificação de objetos do S3 como falso positivo na Proteção contra Malware do S3

Saiba como você pode denunciar possíveis detecções de ameaças de falsos positivos na Proteção contra malware para S3.

Denunciando falsos positivos no Malware Protection for Backup

Saiba como você pode denunciar possíveis detecções de ameaças de falsos positivos no Malware Protection for Backup.

Painel de resumo na Amazon GuardDuty

O painel de GuardDuty resumo fornece uma visão agregada das GuardDuty descobertas geradas em você Conta da AWS no momento Região da AWS.

Se você estiver usando uma conta de GuardDuty administrador, o painel fornece estatísticas e dados agregados para sua conta e contas de membros em sua organização.

Visualização do painel Resumo

1. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.

   GuardDuty exibe o painel Resumo por padrão quando você abre o console.

2. Na página Resumo, escolha o desejado no seletor Região da AWS de região no canto superior direito do console.
3. No menu do seletor de intervalo de datas, escolha o intervalo de datas para o qual você deseja visualizar o resumo. Por padrão, o painel exibe os dados de Hoje.

> **Note**
>
> Se nenhuma descoberta for gerada durante o intervalo de datas selecionado, o painel não terá nenhum dado para exibir. Você pode atualizar o painel ou ajustar o intervalo de datas.

Tópicos

- Visão geral do
- Conclusões
- Tipos de descoberta mais comuns
- Descobertas por gravidade
- Contas com a maioria das descobertas
- Recursos com descobertas
- Descobertas que menos ocorrem
- Cobertura de planos de proteção

Visão geral do

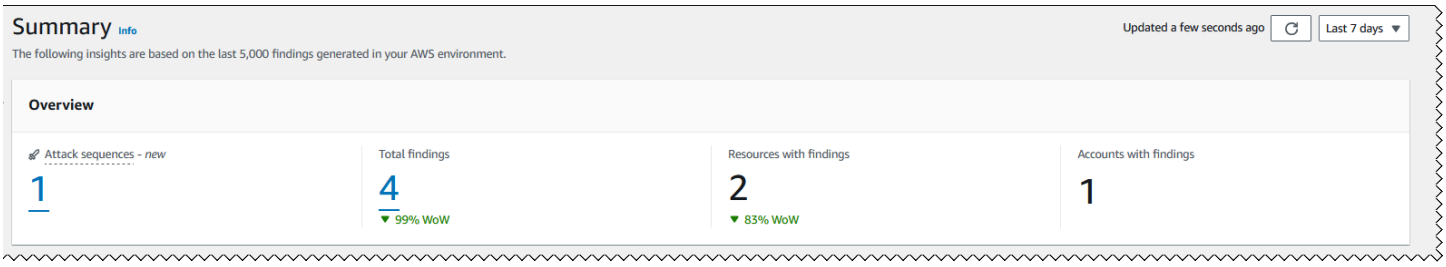
Esta seção fornece os seguintes dados:

- Sequências de ataque: indica o número de descobertas de sequências de ataque GuardDuty geradas em sua conta na região atual.

  GuardDuty detecta possíveis ataques em vários estágios em sua conta. Você pode selecionar o número em Sequências de ataque para ver seus detalhes na página Descobertas.
- Total de descobertas: indica o número total de descobertas geradas em sua conta na região atual. Isso inclui descobertas individuais e descobertas de sequências de ataque.
- Recursos com descobertas: indica o número de recursos associados a uma descoberta e que foram potencialmente comprometidos.

- Contas com descobertas: indica o número de contas nas quais pelo menos uma descoberta foi gerada. Se você for uma conta independente, o valor nesse campo será 1.

Para os intervalos de tempo Últimos 7 dias e Últimos 30 dias, o painel Visão geral pode mostrar a diferença percentual nas descobertas geradas semana após semana (WoW) ou mês a mês (MoM), respectivamente. Se nenhuma descoberta foi gerada na semana ou no mês anterior, sem dados para comparar, a diferença percentual pode não estar disponível.



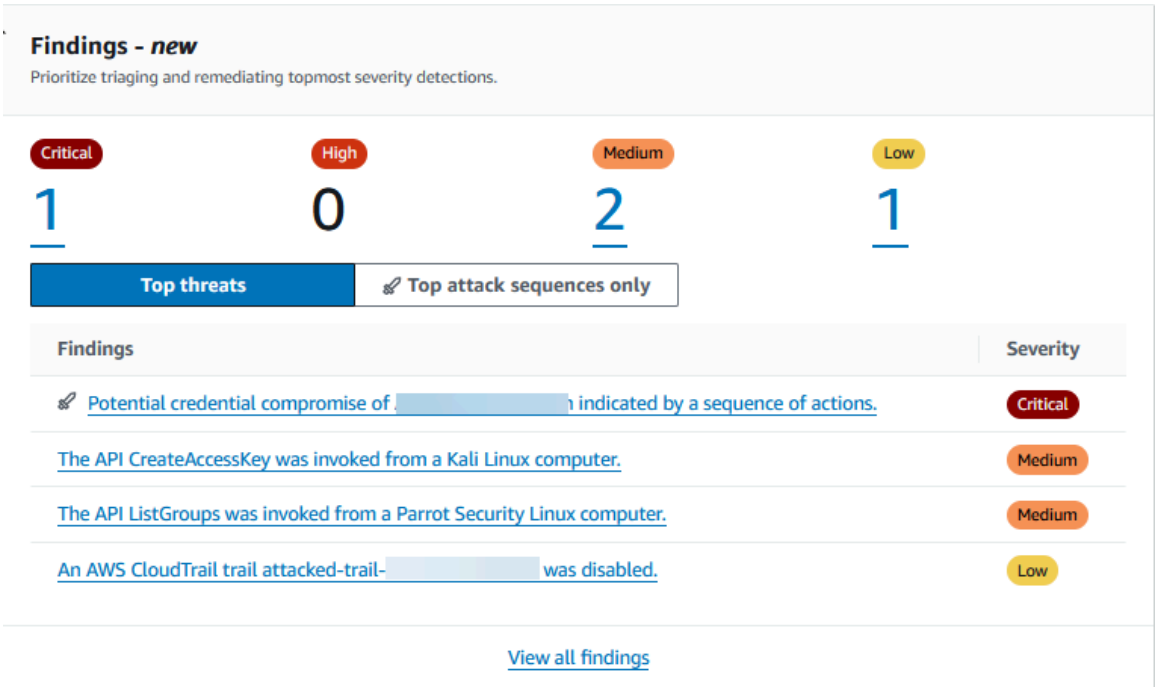
Se você for uma conta de GuardDuty administrador, todos esses campos fornecem os dados resumidos de todas as contas de membros da sua organização.

Conclusões

O widget Descobertas exibe até oito descobertas principais. Essas descobertas são listadas com base em seu nível de gravidade, com as descobertas críticas exibidas primeiro.

Por padrão, é possível visualizar todas as descobertas. Para ver somente os dados das descobertas da sequência de ataque, ative Somente as principais sequências de ataque.

Nessa lista, você pode selecionar qualquer descoberta para visualizar os detalhes.



Tipos de descoberta mais comuns

Esta seção fornece um gráfico de pizza que ilustra os cinco principais tipos de descobertas mais comuns geradas na região atual. Ao passar o mouse sobre cada setor do gráfico de pizza, você pode observar o seguinte:

- Contagem de descobertas: indica o número de vezes que essa descoberta foi gerada no intervalo de datas escolhido.
- Gravidade: indica o nível de gravidade da descoberta.
- Porcentagem: indica a proporção desse tipo de descoberta em relação ao total.
- Última geração: indica quanto tempo passou desde que esse tipo de descoberta foi detectado pela última vez.

Descobertas por gravidade

Esta seção exibe um gráfico de barras mostrando o número total de descobertas no intervalo de datas selecionado. O gráfico divide as descobertas por gravidade (Crítica, Alta, Média e Baixa) e ajuda você a visualizar o número de descobertas em datas específicas dentro do intervalo.

Para ver as contagens de cada nível de gravidade em uma data específica, passe o mouse sobre a barra correspondente no gráfico.

Contas com a maioria das descobertas

Esta seção fornece os seguintes dados:

- Conta: indica o Conta da AWS ID em que a descoberta foi gerada.
- Contagem de descobertas: indica o número de vezes que uma descoberta foi gerada para esse ID de conta.
- Última geração: indica quanto tempo passou desde a última geração de um tipo de descoberta para esse ID de conta.
- Filtro de gravidade: por padrão, os dados são mostrados para os tipos de descoberta de alta gravidade. As opções possíveis para esse campo são Todas as gravidades, gravidade Crítica, gravidade Alta e gravidade Média.

Recursos com descobertas

Esta seção fornece os seguintes dados:

- Recurso: mostra o tipo de recurso potencialmente afetado e, se esse recurso pertencer à sua conta, será possível acessar o link rápido para ver os detalhes do recurso. Se você for uma conta de GuardDuty administrador, poderá ver os detalhes do recurso potencialmente afetado acessando o GuardDuty console com as credenciais da conta do membro proprietário.
- Conta: indica a Conta da AWS ID à qual esse recurso pertence.
- Contagem de descobertas: indica o número de vezes que esse recurso foi associado a uma descoberta.
- Última geração: indica quanto tempo passou desde a última geração de um tipo de descoberta associado a esse recurso.
- Filtro de tipos de recursos: por padrão, os dados são mostrados para todos os tipos de recursos. Ao usar esse filtro, você pode optar por visualizar os dados de um tipo de recurso específico, como Instance AccessKey, Lambda e outros.
- Filtro de gravidade: por padrão, os dados são mostrados para Todas as gravidades. Ao usar esse filtro, é possível optar por visualizar os dados de outros níveis de gravidade. As opções possíveis são gravidade Crítica, gravidade Alta, gravidade Média e Todas as gravidades.

Descobertas que menos ocorrem

Esta seção destaca os tipos de descoberta que ocorrem com pouca frequência em seu AWS ambiente. Esse widget foi projetado para ajudar você a identificar e investigar possíveis padrões de ameaças emergentes.

Esse widget exibe os seguintes dados:

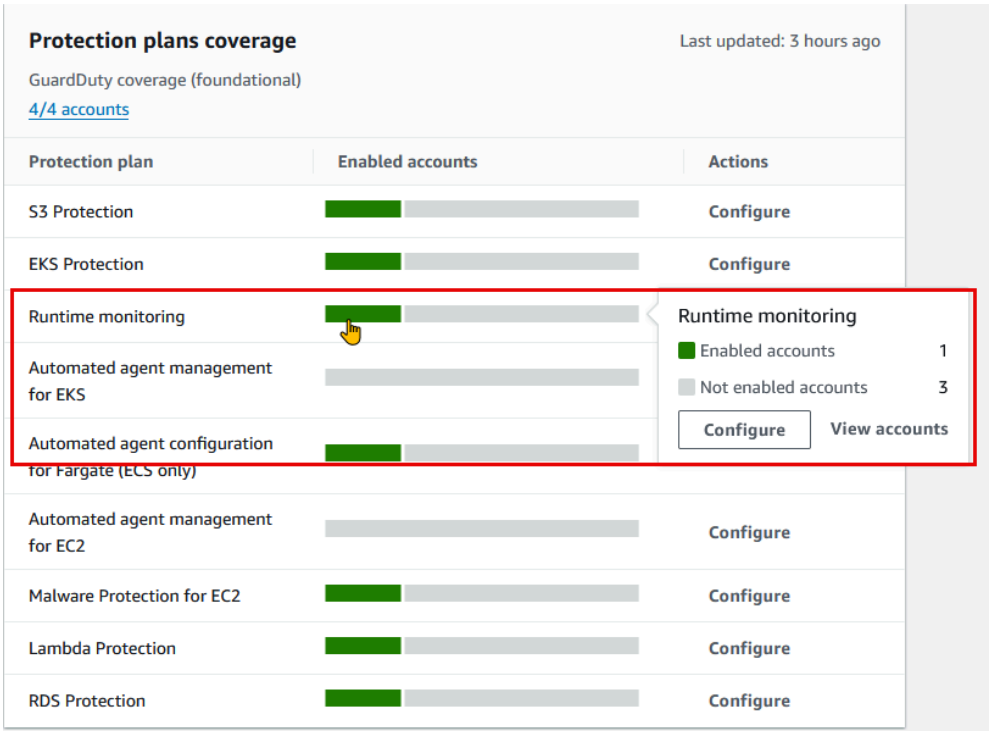
- Tipo de descoberta: indica o nome do tipo de descoberta.
- Contagem de descobertas: indica o número de vezes que esse tipo de descoberta foi gerado no intervalo de tempo escolhido.
- Última geração: indica quanto tempo passou desde que esse tipo de descoberta foi gerado pela última vez.
- Filtro de gravidade: por padrão, os dados são mostrados para os tipos de descoberta de alta gravidade. As opções possíveis para esse campo são gravidade Crítica, gravidade Alta, gravidade Média e Todas as gravidades.

Cobertura de planos de proteção

Esta seção exibe estatísticas de contas de membros da sua organização. Ele mostra o número de contas de membros que foram ativadas GuardDuty (detecção básica de ameaças) na região atual. Somente um GuardDuty administrador delegado pode visualizar as estatísticas das contas dos membros em sua organização. Quando você cria uma nova AWS organização, pode levar até 24 horas para gerar as estatísticas de toda a organização.

Como usar esse widget

- Configuração: se um plano de proteção não estiver configurado, escolha Configurar na coluna Ações.
- Visualizando contas habilitadas: passe o mouse sobre a barra na coluna Contas habilitadas para ver quantas contas habilitaram cada plano de proteção. Para ver mais detalhes da conta, selecione a barra verde e escolha Exibir contas.



Filtrando descobertas em GuardDuty

Um filtro de descoberta permite que você visualize descobertas que correspondam aos critérios especificados e filtre quaisquer descobertas sem correspondência. Você pode criar facilmente filtros de busca usando o GuardDuty console da Amazon ou pode criá-los com a CreateFilterAPI usando JSON. Consulte as seções a seguir para entender como criar um filtro no console. Para usar esses filtros para arquivar automaticamente as descobertas recebidas, consulte Regras de supressão em GuardDuty.

Ao criar filtros, leve em consideração a seguinte lista:

- Você pode especificar no mínimo um atributo ou no máximo 50 atributos como critérios para um determinado filtro.
- Ao usar o operador igual a ou diferente de para filtrar um valor de atributo, como ID da conta, você pode especificar um máximo de 50 valores.
- Cada atributo de critério de filtro é avaliado como um operador `AND`. Vários valores para o mesmo atributo são avaliados como `AND/OR`.
- Para obter informações sobre o número máximo de filtros salvos que você pode criar Conta da AWS em cada um Região da AWS, consulteGuardDuty cotas.

- Os campos abaixo `service.additionalInfo` são especificados usando seu caminho JSON completo, o mesmo que qualquer outro campo. Por exemplo: `{ "service.additionalInfo.sample": { "Equals": ["true"] } }`.
- Os campos de carimbo de data/hora aceitam valores no formato de milissegundos do Unix Epoch (por exemplo,). `1486685375000` Para obter uma lista completa dos campos de carimbo de data/hora, consulte a nota abaixo.

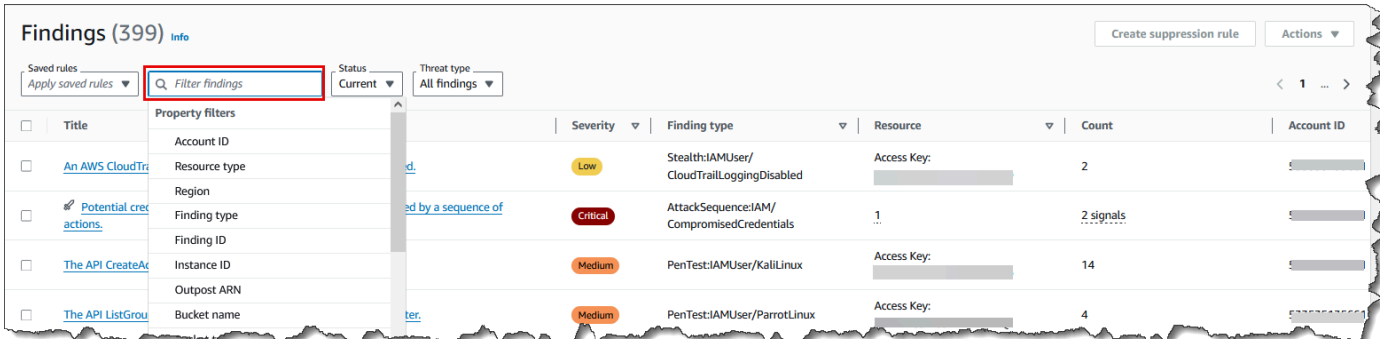
As seções a seguir fornecem instruções sobre como criar e salvar filtros usando o GuardDuty console e os comandos da API e da CLI. Escolha seu método de acesso preferido para continuar.

Criando e salvando o conjunto de filtros no GuardDuty console

Os filtros de localização podem ser criados e testados por meio do GuardDuty console. Os filtros criados pela interface do usuário podem ser salvos para uso em regras de supressão ou em operações futuras de filtro. Um filtro é composto por pelo menos um critério de filtro, que consiste em um atributo de filtro emparelhado com pelo menos um valor.

Para criar e salvar critérios de filtro (console)

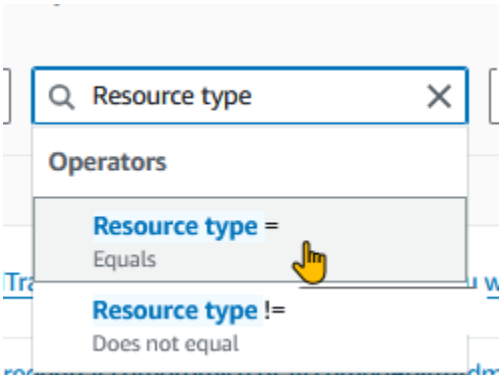
1. Faça login no Console de gerenciamento da AWS e abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.
2. No painel de navegação à esquerda, escolha Descobertas.
3. Na página Descobertas, selecione a barra Filtrar descobertas ao lado do menu Regras salvas. Isso exibirá uma lista expandida de Filtros de propriedades.



4. Na lista expandida de filtros, selecione um atributo com base no qual você deseja filtrar a tabela de descobertas.

   Por exemplo, para ver descobertas sobre as quais o recurso potencialmente afetado é um S3Bucket, escolha Tipo de recurso.

5. Para Operadores, escolha um que ajude você a filtrar as descobertas para obter o resultado desejado. Para continuar o exemplo da etapa anterior, escolha Tipo de recurso =. Isso exibirá uma lista dos tipos de recursos em GuardDuty.



   Se seu caso de uso exigir a exclusão de descobertas específicas, você pode escolher o operador Não é igual ou !=.

6. Especifique o valor do filtro de propriedade selecionado. Se necessário, escolha Aplicar. Para continuar o exemplo da etapa anterior, você pode escolher S3Bucket.

   Isso exibirá as descobertas que correspondem aos filtros aplicados.

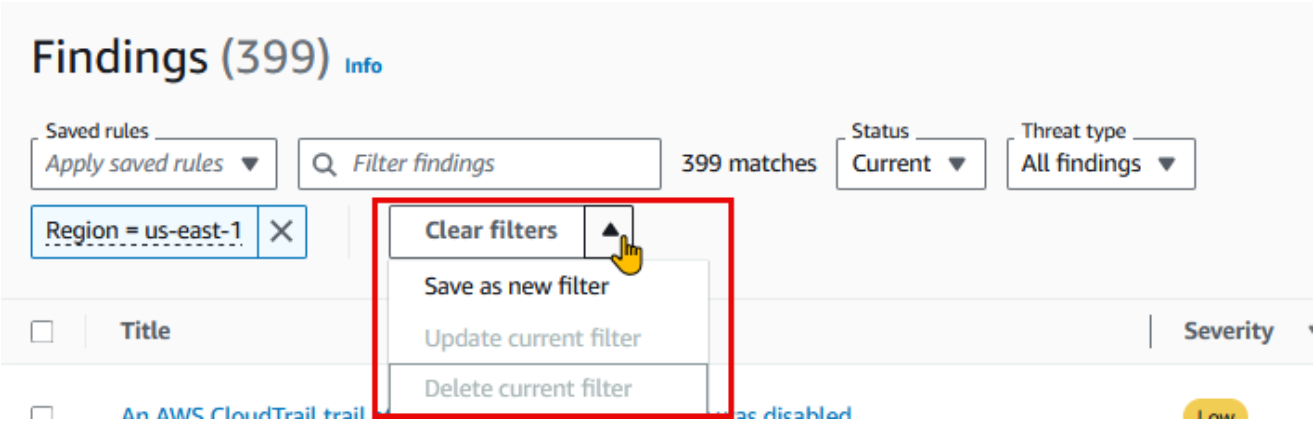
7. Para adicionar mais de um critério de filtro, repita as etapas 3 a 6.

   Para obter uma lista completa de atributos, consulte Filtros de propriedades em GuardDuty.

8. (Opcional) Salve os atributos e valores especificados como filtros.

   Para aplicar essa combinação de filtros novamente no futuro, você pode salvar os atributos especificados e os respectivos valores como um conjunto de filtros.

   a. Depois de criar um critério de filtro com um ou mais filtros de propriedade, selecione a seta no menu Limpar filtros.



b. Insira o nome do conjunto de filtros. O nome deve ter de 3 a 64 caracteres. Os caracteres válidos são a-z A-Z, 0-9, ponto (.), hífen (-) e sublinhado (_).

c. A descrição é opcional. Se você inserir uma descrição, ela pode ter até 512 caracteres.

d. Escolha Criar.

Criação e salvamento do conjunto de filtros usando GuardDuty API e CLI

Você pode criar e testar os filtros de descoberta usando os comandos da API ou da CLI. Um filtro é composto por pelo menos um critério de filtro, que consiste em um atributo de filtro emparelhado com pelo menos um valor. Você pode salvar filtros para criar Regras de supressão ou realizar outras operações de filtro posteriormente.

Para criar filtros de busca usando API/CLI

- Execute a CreateFilterAPI usando o ID do detector regional do Conta da AWS local em que você deseja criar um filtro.

  Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no https://console.aws.amazon.com/guardduty/console ou execute a ListDetectorsAPI.

- Como alternativa, você pode usar a CLI create-filter para criar e salvar o filtro. Você pode usar um ou mais critérios de filtragem dos Filtros de propriedades em GuardDuty.

  Use os exemplos a seguir substituindo os valores de espaço reservado mostrados em vermelho.

  Exemplo 1: crie um novo filtro para visualizar todas as descobertas que correspondem a um tipo específico de descoberta

  O exemplo a seguir cria um filtro que corresponde a todas as descobertas de `PortScan` para uma instância criada com base em uma imagem específica. Os valores do espaço reservado são mostrados em vermelho. Substitua esses valores por valores adequados para sua conta. Por exemplo, *12abc34d567e8fa901bc2d34EXAMPLE* substitua pelo ID do detector regional.

```
aws guardduty create-filter \
--detector-id 12abc34d567e8fa901bc2d34EXAMPLE \
--name FilterExampleName \
--finding-criteria '{"Criterion": {"type": {"Equals": ["Recon:EC2/Portscan"]},
 "resource.instanceDetails.imageId": {"Equals":["ami-0a7a207083example"]}} }'
```

Exemplo 2: crie um novo filtro para visualizar todas as descobertas que correspondem aos níveis de gravidade

O exemplo a seguir cria um filtro que corresponde a todas as descobertas associadas aos níveis de gravidade `HIGH`. Os valores do espaço reservado são mostrados em vermelho. Substitua esses valores por valores adequados para sua conta. Por exemplo, *`12abc34d567e8fa901bc2d34EXAMPLE`* substitua pelo ID do detector regional.

```
aws guardduty create-filter \
--detector-id 12abc34d567e8fa901bc2d34EXAMPLE \
--name FilterExampleName \
--finding-criteria '{"Criterion": {"severity": {"Equals": ["7", "8"]}} }'
```

- Pois API/CLI, Níveis de gravidade das descobertas eles são representados como numerais. Para filtrar as descobertas com base nos níveis de gravidade, use os seguintes valores:
  - Para níveis de gravidade `LOW`, use `{ "severity": { "Equals": ["1", "2", "3"] } }`
  - Para níveis de gravidade `MEDIUM`, use `{ "severity": { "Equals": ["4", "5", "6"] } }`
  - Para níveis de gravidade `HIGH`, use `{ "severity": { "Equals": ["7", "8"] } }`
  - Para níveis de gravidade `CRITICAL`, use `{ "severity": { "Equals": ["9", "10"] } }`
  - Para descobertas com vários níveis de gravidade, use valores de espaço reservado semelhantes ao seguinte exemplo: `{ "severity": { "Equals": ["7", "8", "9", "10"] } }`

  Este exemplo mostrará as descobertas que têm níveis de gravidade `HIGH` ou `CRITICAL`.

  > **Note**
  >
  > Se você especificar um exemplo com apenas um valor numérico em vez de todos os valores numéricos associados a um nível de gravidade, a API e a CLI poderão mostrar as descobertas filtradas. Quando você usa esse conjunto de filtros salvo no GuardDuty console, ele não funcionará conforme o esperado. Isso ocorre porque o GuardDuty console considera os valores do filtro como `CRITICAL HIGHMEDIUM`,, `LOW` e. Por exemplo, espera-se que um filtro criado com um comando CLI que `{ "severity": { "Equals": ["9"] } }` inclua mostre uma saída apropriada em. API/CLI No entanto, esse filtro salvo inclui um nível de severidade parcial quando usado no

GuardDuty console e não mostrará uma saída esperada. Isso torna necessário que a API e a CLI especifiquem todos os valores associados a cada nível de gravidade.

Filtrar metadados do ciclo de vida

Ao recuperar detalhes do filtro usando a GetFilterAPI, você pode visualizar os campos de metadados do ciclo de vida. Esses campos mostram quando um filtro foi criado e quantas vezes ele foi modificado.

A GetFilter resposta inclui os seguintes campos de metadados do ciclo de vida:

`createdAt`

O carimbo de data e hora em que o filtro foi criado originalmente. GuardDuty define esse valor no momento da criação e nunca o altera. GuardDuty não preenche esse campo para filtros legados (filtros que você criou antes do lançamento desse recurso).

`updatedAt`

A data e hora da última atualização do filtro. GuardDuty atualiza esse valor em cada UpdateFilterchamada bem-sucedida. Na hora da criação, `updatedAt` partidas`createdAt`. Para filtros legados, esse campo aparece somente depois que você atualiza o filtro pelo menos uma vez.

`version`

Um número inteiro que conta quantas vezes você modificou o filtro. Começa em 1 quando você cria o filtro e aumenta em 1 a cada UpdateFilter chamada bem-sucedida, independentemente de o conteúdo do filtro mudar. GuardDuty não preenche esse campo para filtros legados.

> **Note**
>
> Esses campos de metadados do ciclo de vida são somente para leitura. As UpdateFilter operações CreateFilter e não aceitam esses campos como entrada e suas respostas não incluem esses campos. Para ver os metadados do ciclo de vida, ligue para. GetFilter

Filtros de propriedades em GuardDuty

Ao criar filtros ou classificar descobertas usando as operações da API, você deve especificar critérios de filtro em JSON. Esses critérios de filtro se correlacionam com o JSON dos detalhes de uma descoberta. A tabela a seguir contém uma lista dos nomes de exibição do console para atributos de filtro e seus nomes de campo JSON equivalentes.

Nome do campo do console	Nome do campo JSON
ID da conta	accountId
ID da descoberta	id
Região	region
Gravidade	severidade Para filtrar os tipos de descoberta com base no nível de gravidade dos tipos de descobert a. Para obter mais informações sobre valores de severidade, consulte Níveis de severidad e das GuardDuty descobertas. Se você usa `severity` com API, AWS CLI, ou CloudForm ation, é atribuído um valor numérico. Para obter mais informações, consulte FindingCriteria na Amazon GuardDuty API Reference.
Tipo de descoberta	type
Nome da regra de detecção personalizada	personalizado DetectionRuleName Presente somente nas descobertas geradas por uma regra de detecção personalizada do Runtime Monitoring. Para obter mais informações, consulte Conclusões das regras de monitoramento de tempo de execução.
Atualizado em	updatedAt

Nome do campo do console	Nome do campo JSON
Access Key ID	acesso ao recurso KeyDetails.accessKeyId
Principal ID	acesso ao recurso KeyDetails.principalId
Nome de usuário	acesso ao recurso KeyDetails.userName
Tipo de usuário	acesso ao recurso KeyDetails.userType
ID do perfil da instância do IAM	recurso.instância Details.iamInstanceProfile.id
ID da instância	recurso.instância Details.instanceId
ID da imagem da instância	recurso.instância Details.imageId
Chave de tag da instância	recurso.instância Details.tags.key
Valor de tag da instância	recurso.instância Details.tags.value
Endereço IPv6	recurso.instância Details.networkInterfaces.ipv6Addresses
Endereço IPv4 privado	recurso.instância Details.networkInterfaces.privateIpAddresses.privateIpAddress
Nome público do DNS	recurso.instância Details.networkInterfaces.publicDnsName
IP público	recurso.instância Details.networkInterfaces.publicIp
ID do grupo de segurança	recurso.instância Details.networkInterfaces.securityGroups.groupId
Nome do security group	recurso.instância Details.networkInterfaces.securityGroups.groupName
ID da sub-rede	recurso.instância Details.networkInterfaces.subnetId

Nome do campo do console	Nome do campo JSON
ID da VPC	recurso.instância Details.networkInterfaces.vpcId
ARN do Outpost	recurso.instância Details.outpostARN
Tipo de atributo	resource.resourceType
Permissões do bucket	recursos.3 BucketDetails.publicAccess.effectivePermission
Nome do bucket	recursos.3 BucketDetails.name
Bucket tag key	recursos.3 BucketDetails.tags.key
Bucket tag value	recursos.3 BucketDetails.tags.value
Tipo de bucket	recursos.3 BucketDetails.type
Tipo de ação	service.action.actionType
API chamada	service.action.aws ApiCallAction.api
Tipo de chamador da API	service.action.aws ApiCallAction.callerType
Códigos de erro da API	service.action.aws ApiCallAction.errorCode
Cidade do chamador da API	service.action.aws ApiCallAction.remoteIpDetails.city.cityName
País do chamador da API	service.action.aws ApiCallAction.remoteIpDetails.country.countryName
Endereço IPv4 do chamador da API	service.action.aws ApiCallAction.remoteIpDetails.ipAddressV4
Endereço IPv6 do chamador da API	service.action.aws ApiCallAction.remoteIpDetails.ipAddressV6

Nome do campo do console	Nome do campo JSON
ID de ASN do chamador da API	service.action.aws ApiCallAction.remoteIpDetails.organization.asn
Nome de ASN do chamador da API	service.action.aws ApiCallAction.remoteIpDetails.organization.asnOrg
Nome do serviço de chamador da API	service.action.aws ApiCallAction.serviceName
Domínio de solicitação de DNS	service.action.dns RequestAction.domain
Sufixo de domínio de solicitação de DNS	service.action.dns RequestAction.domainWithSuffix
Conexão de rede bloqueada	service.action.network ConnectionAction.blocked
Direção de conexão de rede	service.action.network ConnectionAction.connectionDirection
Porta local de conexão de rede	service.action.network ConnectionAction.localPortDetails.port
Protocolo de conexão de rede	service.action.network ConnectionAction.protocol
Cidade de conexão de rede	service.action.network ConnectionAction.remoteIpDetails.city.cityName
País de conexão de rede	service.action.network ConnectionAction.remoteIpDetails.country.countryName
Endereço IPv4 remoto de conexão de rede	service.action.network ConnectionAction.remoteIpDetails.ipAddressV4
Endereço IPv6 remoto de conexão de rede	service.action.network ConnectionAction.remoteIpDetails.ipAddressV6

Nome do campo do console	Nome do campo JSON
ID de ASN do IP remoto de conexão de rede	service.action.network ConnectionAction.remoteIpDetails.organization.asn
Nome de ASN do IP remoto de conexão de rede	service.action.network ConnectionAction.remoteIpDetails.organization.asnOrg
Porta remota de conexão de rede	service.action.network ConnectionAction.remotePortDetails.port
Conta remota afiliada	service.action.aws ApiCallAction.remoteAccountDetails.affiliated
Endereço IPv4 do chamador da API do Kubernetes	service.action.kubernetes ApiCallAction.remoteIpDetails.ipAddressV4
Endereço IPv6 do chamador da API do Kubernetes	service.action.kubernetes ApiCallAction.remoteIpDetails.ipAddressV6
Namespace do Kubernetes	service.action.kubernetes ApiCallAction.namespace
ID ASN do chamador da API Kubernetes	service.action.kubernetes ApiCallAction.remoteIpDetails.organization.asn
URI de solicitação de chamada de API do Kubernetes	service.action.kubernetes ApiCallAction.requestUri
Código de status da API do Kubernetes	service.action.kubernetes ApiCallAction.statusCode
Endereço IPv4 local da conexão de rede	service.action.network ConnectionAction.localIpDetails.ipAddressV4
Endereço IPv6 local da conexão de rede	service.action.network ConnectionAction.localIpDetails.ipAddressV6
Protocolo	service.action.network ConnectionAction.protocol

Nome do campo do console	Nome do campo JSON
Nome do serviço de chamada de API	service.action.aws ApiCallAction.serviceName
ID da conta do chamador da API	service.action.aws ApiCallAction.remoteAccountDetails.accountId
Nome da lista de ameaças	serviço.adicional Info.threatListName
Função do recurso	service.resourceRole
Nome do cluster do EKS	resource.eks ClusterDetails.name
Nome da workload do Kubernetes	recurso.kubernetes Details.kubernetes WorkloadDetails.name
Namespace de workload do Kubernetes	recurso.kubernetes Details.kubernetes WorkloadDetails.namespace
Nome de usuário do Kubernetes	recurso.kubernetes Details.kubernetes UserDetails.username
Imagem de contêiner do Kubernetes	recurso.kubernetes Details.kubernetes WorkloadDetails.containers.image
Prefixo de imagens de contêiner do Kubernetes	recurso.kubernetes Details.kubernetes WorkloadDetails.containers.imagePrefix
ID de verificação	service.ebs VolumeScanDetails.scanId
Nome da ameaça de escaneamento de volume do EBS	service.ebs VolumeScanDetails.scanDetections.threatDetectedByName.threatNames.name
Nome da ameaça de verificação do objeto do S3	serviço.malware ScanDetails.threats.name
Gravidade da ameaça	service.ebs VolumeScanDetails.scanDetections.threatDetectedByName.threatNames.severity

Nome do campo do console	Nome do campo JSON
Arquivo SHA	service.ebs VolumeScanDetails.scanDetections.threatDetectedByName.threatNames.filePaths.hash
Nome do cluster do ECS	recurso.ecs ClusterDetails.name
Imagens de contêiner do ECS	recurso.ecs ClusterDetails.taskDetails.containers.image
ARN da definição de tarefas do ECS	recurso.ecs ClusterDetails.taskDetails.definitionArn
Imagem de contêiner autônoma	resource.container Details.image
ID da instância de banco de dados	resource.rds DbInstanceDetails.dbInstanceIdentifier
ID do cluster de banco de dados	resource.rds DbInstanceDetails.dbClusterIdentifier
Mecanismo do banco de dados	resource.rds DbInstanceDetails.engine
Usuário do banco de dados	resource.rds DbUserDetails.user
Executável SHA-256	service.runtime Details.process.executableSha256
Nome do processo	service.runtime Details.process.name
Caminho executável	service.runtime Details.process.executablePath
Nome de função do Lambda	recurso.lambda Details.functionName
ARN da função do Lambda.	recurso.lambda Details.functionArn
Chave de tags de funções do Lambda	recurso.lambda Details.tags.key
Valor de tags de funções do Lambda	recurso.lambda Details.tags.value

Nome do campo do console	Nome do campo JSON
Domínio de solicitação de DNS	service.action.dns RequestAction.domainWithSuffix

Todos os outros campos de busca (listados abaixo) estão disponíveis somente como critérios de filtro da regra de supressão (usando CreateFiltere UpdateFilter). Esses campos não são compatíveis com outras operações de API. As regras de supressão que usam esses campos devem ser criadas ou atualizadas por meio da API. Esses campos só podem ser aplicados para filtros com uma `ARCHIVE` ação.

> **Note**
>
> Os campos a seguir aceitam valores de timestamp no formato de milissegundos do Unix Epoch (por exemplo, `1262309025000` representa sexta-feira, 1º de janeiro de 2010 às 1:23:45 GMT):
>
> - createdAt
> - updatedAt
> - serviço.evento FirstSeen
> - serviço.evento LastSeen
> - recurso.instância Details.launchTime
> - recurso.lambda Details.lastModifiedAt
> - recursos.3 BucketDetails.createdAt
> - resource.eks ClusterDetails.createdAt
> - recurso.ecs ClusterDetails.taskDetails.createdAt
> - recurso.ecs ClusterDetails.taskDetails.startedAt
> - service.ebs VolumeScanDetails.scanStartedAt
> - service.ebs VolumeScanDetails.scanCompletedAt
> - service.runtime Details.context.modifiedAt
> - service.runtime Details.context.modifyingProcess.startTime
> - service.runtime Details.context.modifyingProcess.lineage.startTime
> - service.runtime Details.context.targetProcess.startTime
> - service.runtime Details.context.targetProcess.lineage.startTime
> - service.runtime Details.process.startTime
> - service.runtime Details.process.lineage.startTime
> - service.detection.sequence.actors.session.createdTime

- service.detection.sequence.signals.criado em
- service.detection.sequence.signals.Atualizado em
- service.detection.sequence.signals.first SeenAt
- service.detection.sequence.signals.last SeenAt
- service.detection.sequence.resources.data.s3 Bucket.createdAt
- service.detection.sequence.resources.data.ecs Task.createdAt
- service.detection.sequence.resources.data.eks Cluster.createdAt

Nome do campo JSON
arn
associado AttackSequenceArn
createdAt
Partição
acesso ao recurso KeyDetails.userIdentity.accessKeyId
acesso ao recurso KeyDetails.userIdentity.accountId
acesso ao recurso KeyDetails.userIdentity.arn
acesso ao recurso KeyDetails.userIdentity.principalId
acesso ao recurso KeyDetails.userIdentity.sessionContext.attributes.mfaAuthenticated
acesso ao recurso KeyDetails.userIdentity.sessionContext.ec2RoleDelivery
acesso ao recurso KeyDetails.userIdentity.sessionContext.invokedBy
acesso ao recurso KeyDetails.userIdentity.sessionContext.sessionIssuer.accountId
acesso ao recurso KeyDetails.userIdentity.sessionContext.sessionIssuer.arn
acesso ao recurso KeyDetails.userIdentity.sessionContext.sessionIssuer.principalId
acesso ao recurso KeyDetails.userIdentity.sessionContext.sessionIssuer.type

Nome do campo JSON
acesso ao recurso KeyDetails.userIdentity.sessionContext.sessionIssuer.userName
acesso ao recurso KeyDetails.userIdentity.sessionContext.sourceIdentity
acesso ao recurso KeyDetails.userIdentity.sessionContext.webIdFederationData.attributes
acesso ao recurso KeyDetails.userIdentity.sessionContext.webIdFederationData.federatedProvider
acesso ao recurso KeyDetails.userIdentity.type
acesso ao recurso KeyDetails.userIdentity.userName
recurso.alicerce GuardrailDetails.guardrailArn
recurso.alicerce GuardrailDetails.guardrailVersion
resource.container Details.containerRuntime
resource.container Details.imagePrefix
resource.container Details.securityContext.allowPrivilegeEscalation
resource.container Details.securityContext.privileged
resource.container Details.volumeMounts.mountPath
resource.container Details.volumeMounts.name
resource.ebs VolumeDetails.scannedVolumeDetails.deviceName
resource.ebs VolumeDetails.scannedVolumeDetails.encryptionType
resource.ebs VolumeDetails.scannedVolumeDetails.kmsKeyArn
resource.ebs VolumeDetails.scannedVolumeDetails.snapshotArn
resource.ebs VolumeDetails.scannedVolumeDetails.volumeArn
resource.ebs VolumeDetails.scannedVolumeDetails.volumeSizeInGB

Nome do campo JSON
resource.ebs VolumeDetails.scannedVolumeDetails.volumeType
resource.ebs VolumeDetails.skippedVolumeDetails.deviceName
resource.ebs VolumeDetails.skippedVolumeDetails.encryptionType
resource.ebs VolumeDetails.skippedVolumeDetails.kmsKeyArn
resource.ebs VolumeDetails.skippedVolumeDetails.snapshotArn
resource.ebs VolumeDetails.skippedVolumeDetails.volumeArn
resource.ebs VolumeDetails.skippedVolumeDetails.volumeSizeInGB
resource.ebs VolumeDetails.skippedVolumeDetails.volumeType
recurso.ecs ClusterDetails.activeServicesCount
recurso.ecs ClusterDetails.arn
recurso.ecs ClusterDetails.registeredContainerInstancesCount
recurso.ecs ClusterDetails.runningTasksCount
recurso.ecs ClusterDetails.status
recurso.ecs ClusterDetails.tags.key
recurso.ecs ClusterDetails.tags.value
recurso.ecs ClusterDetails.taskDetails.arn
recurso.ecs ClusterDetails.taskDetails.containers.containerRuntime
recurso.ecs ClusterDetails.taskDetails.containers.id
recurso.ecs ClusterDetails.taskDetails.containers.imagePrefix
recurso.ecs ClusterDetails.taskDetails.containers.name

Nome do campo JSON
recurso.ecs ClusterDetails.taskDetails.containers.securityContext.allowPrivilegeEscalation
recurso.ecs ClusterDetails.taskDetails.containers.securityContext.privileged
recurso.ecs ClusterDetails.taskDetails.containers.volumeMounts.mountPath
recurso.ecs ClusterDetails.taskDetails.containers.volumeMounts.name
recurso.ecs ClusterDetails.taskDetails.createdAt
recurso.ecs ClusterDetails.taskDetails.group
recurso.ecs ClusterDetails.taskDetails.launchType
recurso.ecs ClusterDetails.taskDetails.startedAt
recurso.ecs ClusterDetails.taskDetails.startedBy
recurso.ecs ClusterDetails.taskDetails.tags.key
recurso.ecs ClusterDetails.taskDetails.tags.value
recurso.ecs ClusterDetails.taskDetails.version
recurso.ecs ClusterDetails.taskDetails.volumes.hostPath.path
recurso.ecs ClusterDetails.taskDetails.volumes.name
resource.eks ClusterDetails.arn
resource.eks ClusterDetails.createdAt
resource.eks ClusterDetails.status
resource.eks ClusterDetails.tags.key
resource.eks ClusterDetails.tags.value
resource.eks ClusterDetails.vpcId

Nome do campo JSON
recurso.instância Details.iamInstanceProfile.arn
recurso.instância Details.instanceState
recurso.instância Details.instanceType
recurso.instância Details.launchTime
recurso.instância Details.networkInterfaces.networkInterfaceId
recurso.instância Details.networkInterfaces.privateDnsName
recurso.instância Details.networkInterfaces.privateIpAddress
recurso.instância Details.networkInterfaces.privateIpAddresses.privateDnsName
recurso.instância Details.platform
recurso.instância Details.productCodes.productCodeId
recurso.instância Details.productCodes.productCodeType
recurso.kubernetes Details.kubernetesUserDetails.groups
recurso.kubernetes Details.kubernetesUserDetails.impersonatedUser.groups
recurso.kubernetes Details.kubernetesUserDetails.impersonatedUser.username
recurso.kubernetes Details.kubernetesUserDetails.sessionName
recurso.kubernetes Details.kubernetesUserDetails.uid
recurso.kubernetes Details.kubernetesWorkloadDetails.containers.containerRuntime
recurso.kubernetes Details.kubernetesWorkloadDetails.containers.id
recurso.kubernetes Details.kubernetesWorkloadDetails.containers.name
recurso.kubernetes Details.kubernetesWorkloadDetails.containers.securityContext.allowPrivilegeEscalation

Nome do campo JSON
recurso.kubernetes Details.kubernetesWorkloadDetails.containers.securityContext.privileged
recurso.kubernetes Details.kubernetesWorkloadDetails.containers.volumeMounts.mountPath
recurso.kubernetes Details.kubernetesWorkloadDetails.containers.volumeMounts.name
recurso.kubernetes Details.kubernetesWorkloadDetails.hostIpc
recurso.kubernetes Details.kubernetesWorkloadDetails.hostNetwork
recurso.kubernetes Details.kubernetesWorkloadDetails.hostPid
recurso.kubernetes Details.kubernetesWorkloadDetails.serviceAccountName
recurso.kubernetes Details.kubernetesWorkloadDetails.type
recurso.kubernetes Details.kubernetesWorkloadDetails.uid
recurso.kubernetes Details.kubernetesWorkloadDetails.volumes.hostPath.path
recurso.kubernetes Details.kubernetesWorkloadDetails.volumes.name
recurso.lambda Details.description
recurso.lambda Details.lastModifiedAt
recurso.lambda Details.revisionId
recurso.lambda Details.vpcConfig.securityGroups.groupId
recurso.lambda Details.vpcConfig.securityGroups.groupName
recurso.lambda Details.vpcConfig.subnetIds
recurso.lambda Details.vpcConfig.vpcId
resource.rds DbInstanceDetails.dbInstanceArn
resource.rds DbInstanceDetails.dbiResourceId

Nome do campo JSON
resource.rds DbInstanceDetails.dbSecurityGroups.name
resource.rds DbInstanceDetails.dbSecurityGroups.status
resource.rds DbInstanceDetails.engineVersion
resource.rds DbInstanceDetails.iamDatabaseAuthenticationEnabled
resource.rds DbInstanceDetails.publiclyAccessible
resource.rds DbInstanceDetails.vpcId
resource.rds DbInstanceDetails.vpcSecurityGroups.status
resource.rds DbInstanceDetails.vpcSecurityGroups.vpcSecurityGroupId
resource.rds DbUserDetails.application
resource.rds DbUserDetails.authMethod
resource.rds DbUserDetails.database
resource.rds DbUserDetails.ssl
resource.rds LimitlessDbDetails.dbClusterIdentifier
resource.rds LimitlessDbDetails.dbShardGroupArn
resource.rds LimitlessDbDetails.dbShardGroupIdentifier
resource.rds LimitlessDbDetails.dbShardGroupResourceId
resource.rds LimitlessDbDetails.engine
resource.rds LimitlessDbDetails.engineVersion
resource.rds LimitlessDbDetails.tags.key
resource.rds LimitlessDbDetails.tags.value

Nome do campo JSON
recursos.3 BucketDetails.arn
recursos.3 BucketDetails.createdAt
recursos.3 BucketDetails.defaultServerSideEncryption.encryptionType
recursos.3 BucketDetails.defaultServerSideEncryption.kmsMasterKeyArn
recursos.3 BucketDetails.owner.id
recursos.3 BucketDetails.publicAccess.permissionConfiguration.accountLevelPermissions.blockPublicAccess.blockPublicAcls
recursos.3 BucketDetails.publicAccess.permissionConfiguration.accountLevelPermissions.blockPublicAccess.blockPublicPolicy
recursos.3 BucketDetails.publicAccess.permissionConfiguration.accountLevelPermissions.blockPublicAccess.ignorePublicAcls
recursos.3 BucketDetails.publicAccess.permissionConfiguration.accountLevelPermissions.blockPublicAccess.restrictPublicBuckets
recursos.3 BucketDetails.publicAccess.permissionConfiguration.bucketLevelPermissions.accessControlList.allowsPublicReadAccess
recursos.3 BucketDetails.publicAccess.permissionConfiguration.bucketLevelPermissions.accessControlList.allowsPublicWriteAccess
recursos.3 BucketDetails.publicAccess.permissionConfiguration.bucketLevelPermissions.blockPublicAccess.blockPublicAcls
recursos.3 BucketDetails.publicAccess.permissionConfiguration.bucketLevelPermissions.blockPublicAccess.blockPublicPolicy
recursos.3 BucketDetails.publicAccess.permissionConfiguration.bucketLevelPermissions.blockPublicAccess.ignorePublicAcls

Nome do campo JSON
recursos.3 BucketDetails.publicAccess.permissionConfiguration.bucketLevelPermissions.blockPublicAccess.restrictPublicBuckets
recursos.3 BucketDetails.publicAccess.permissionConfiguration.bucketLevelPermissions.bucketPolicy.allowsPublicReadAccess
recursos.3 BucketDetails.publicAccess.permissionConfiguration.bucketLevelPermissions.bucketPolicy.allowsPublicWriteAccess
recursos.3 BucketDetails.s3ObjectDetails.eTag
recursos.3 BucketDetails.s3ObjectDetails.hash
recursos.3 BucketDetails.s3ObjectDetails.key
recursos.3 BucketDetails.s3ObjectDetails.objectArn
recursos.3 BucketDetails.s3ObjectDetails.versionId
schemaVersion
service.action.aws ApiCallAction.domainDetails.domain
service.action.aws ApiCallAction.remoteIpDetails.country.countryCode
service.action.aws ApiCallAction.remoteIpDetails.geoLocation.lat
service.action.aws ApiCallAction.remoteIpDetails.geoLocation.lon
service.action.aws ApiCallAction.remoteIpDetails.organization.isp
service.action.aws ApiCallAction.remoteIpDetails.organization.org
service.action.aws ApiCallAction.userAgent
service.action.dns RequestAction.blocked
service.action.dns RequestAction.protocol
service.action.kubernetes ApiCallAction.parameters

Nome do campo JSON
service.action.kubernetes ApiCallAction.remoteIpDetails.country.countryCode
service.action.kubernetes ApiCallAction.remoteIpDetails.geoLocation.lat
service.action.kubernetes ApiCallAction.remoteIpDetails.geoLocation.lon
service.action.kubernetes ApiCallAction.resource
service.action.kubernetes ApiCallAction.resourceName
service.action.kubernetes ApiCallAction.sourceIPs
service.action.kubernetes ApiCallAction.subresource
service.action.kubernetes ApiCallAction.userAgent
service.action.kubernetes ApiCallAction.verb
service.action.kubernetes PermissionCheckedDetails.allowed
service.action.kubernetes PermissionCheckedDetails.namespace
service.action.kubernetes PermissionCheckedDetails.resource
service.action.kubernetes PermissionCheckedDetails.verb
service.action.kubernetes RoleBindingDetails.kind
service.action.kubernetes RoleBindingDetails.name
service.action.kubernetes RoleBindingDetails.roleRefKind
service.action.kubernetes RoleBindingDetails.roleRefName
service.action.kubernetes RoleBindingDetails.uid
service.action.kubernetes RoleDetails.kind
service.action.kubernetes RoleDetails.name

Nome do campo JSON
service.action.kubernetes RoleDetails.uid
service.action.network ConnectionAction.localNetworkInterface
service.action.network ConnectionAction.localPortDetails.portName
service.action.network ConnectionAction.remoteIpDetails.country.countryCode
service.action.network ConnectionAction.remoteIpDetails.geoLocation.lat
service.action.network ConnectionAction.remoteIpDetails.geoLocation.lon
service.action.network ConnectionAction.remoteIpDetails.organization.isp
service.action.network ConnectionAction.remoteIpDetails.organization.org
service.action.network ConnectionAction.remotePortDetails.portName
service.action.port ProbeAction.blocked
service.action.port ProbeAction.portProbeDetails.localIpDetails.ipAddressV4
service.action.port ProbeAction.portProbeDetails.localIpDetails.ipAddressV6
service.action.port ProbeAction.portProbeDetails.localPortDetails.port
service.action.port ProbeAction.portProbeDetails.localPortDetails.portName
service.action.port ProbeAction.portProbeDetails.remoteIpDetails.city.cityName
service.action.port ProbeAction.portProbeDetails.remoteIpDetails.country.countryCode
service.action.port ProbeAction.portProbeDetails.remoteIpDetails.country.countryName
service.action.port ProbeAction.portProbeDetails.remoteIpDetails.geoLocation.lat
service.action.port ProbeAction.portProbeDetails.remoteIpDetails.geoLocation.lon
service.action.port ProbeAction.portProbeDetails.remoteIpDetails.ipAddressV4

Nome do campo JSON
service.action.port ProbeAction.portProbeDetails.remoteIpDetails.ipAddressV6
service.action.port ProbeAction.portProbeDetails.remoteIpDetails.organization.asn
service.action.port ProbeAction.portProbeDetails.remoteIpDetails.organization.asnOrg
service.action.port ProbeAction.portProbeDetails.remoteIpDetails.organization.isp
service.action.port ProbeAction.portProbeDetails.remoteIpDetails.organization.org
service.action.rds LoginAttemptAction.loginAttributes.application
service.action.rds LoginAttemptAction.loginAttributes.failedLoginAttempts
service.action.rds LoginAttemptAction.loginAttributes.successfulLoginAttempts
service.action.rds LoginAttemptAction.loginAttributes.user
service.action.rds LoginAttemptAction.remoteIpDetails.city.cityName
service.action.rds LoginAttemptAction.remoteIpDetails.country.countryCode
service.action.rds LoginAttemptAction.remoteIpDetails.country.countryName
service.action.rds LoginAttemptAction.remoteIpDetails.geoLocation.lat
service.action.rds LoginAttemptAction.remoteIpDetails.geoLocation.lon
service.action.rds LoginAttemptAction.remoteIpDetails.ipAddressV4
service.action.rds LoginAttemptAction.remoteIpDetails.ipAddressV6
service.action.rds LoginAttemptAction.remoteIpDetails.organization.asn
service.action.rds LoginAttemptAction.remoteIpDetails.organization.asnOrg
service.action.rds LoginAttemptAction.remoteIpDetails.organization.isp
service.action.rds LoginAttemptAction.remoteIpDetails.organization.org

Nome do campo JSON
serviço.adicional Info.agentDetails.agentId
serviço.adicional Info.agentDetails.agentVersion
serviço.adicional Info.anomalies.anomalousAPIs
serviço.adicional Info.authenticationMethod
serviço.adicional Info.averagePacketSizeIn
serviço.adicional Info.averagePacketSizeOut
serviço.adicional Info.context
serviço.adicional Info.domain
serviço.adicional Info.inBytes
serviço.adicional Info.localNetworkInterfaceOwner
serviço.adicional Info.localPort
serviço.adicional Info.outBytes
serviço.adicional Info.packetsIn
serviço.adicional Info.packetsOut
serviço.adicional Info.policyArn
serviço.adicional Info.policyName
serviço.adicional Info.remotePort
serviço.adicional Info.sample
serviço.adicional Info.scannedPort
serviço.adicional Info.threatFileSha256

Nome do campo JSON
serviço.adicional Info.threatName
serviço.adicional Info.totalBytesIn
serviço.adicional Info.totalBytesOut
serviço.adicional Info.type
serviço.adicional Info.unusual.asnOrg
serviço.adicional Info.unusual.port
serviço.adicional Info.unusualProtocol
serviço.adicional Info.userAgent.fullUserAgent
serviço.adicional Info.userAgent.userAgentCategory
serviço.adicional Info.value
serviço.adicional Info.vpcOwnerAccountId
service.count
service.detection.sequence.actors.id
service.detection.sequence.actors.process.name
service.detection.sequence.actors.process.path
service.detection.sequence.actors.process.sha256
service.detection.sequence.actors.session.createdTime
service.detection.sequence.actors.session.issuer
service.detection.sequence.actors.session.mfaStatus
service.detection.sequence.actors.session.uid

Nome do campo JSON
service.detection.sequence.actors.user.account.account
service.detection.sequence.actors.user.account.uid
service.detection.sequence.actors.user.credentialUid
service.detection.sequence.actors.user.name
service.detection.sequence.actors.user.type
service.detection.sequence.actors.user.uid
service.detection.sequence.additional SequenceTypes
service.detection.sequence.description
service.detection.sequence.endpoints.autonomous System.name
service.detection.sequence.endpoints.autonomous System.number
service.detection.sequence.endpoints.connection.direction
service.detection.sequence.endpoints.domain
service.detection.sequence.endpoints.id
service.detection.sequence.endpoints.ip
service.detection.sequence.endpoints.location.city
service.detection.sequence.endpoints.location.country
service.detection.sequence.endpoints.location.lat
service.detection.sequence.endpoints.location.lon
service.detection.sequence.endpoints.port
service.detection.sequence.resources.AccountId

Nome do campo JSON
service.detection.sequence.resources.cloudPartition
service.detection.sequence.resources.data.access Key.principalId
service.detection.sequence.resources.data.access Key.userName
service.detection.sequence.resources.data.access Key.userType
service.detection.sequence.resources.data.autoscaling AutoScalingGroup.ec2InstanceUids
service.detection.sequence.resources.data.cloudformation Stack.ec2InstanceUids
service.detection.sequence.resources.data.container.image
service.detection.sequence.resources.data.container.ImageUID
service.detection.sequence.resources.data.ec2 Image.ec2InstanceUids
service.detection.sequence.resources.data.ec2 Instance.availabilityZone
service.detection.sequence.resources.data.ec2 Instance.ec2NetworkInterfaceUids
service.detection.sequence.resources.data.ec2 Instance.iamInstanceProfile.arn
service.detection.sequence.resources.data.ec2 Instance.iamInstanceProfile.id
service.detection.sequence.resources.data.ec2 Instance.imageDescription
service.detection.sequence.resources.data.ec2 Instance.instanceState
service.detection.sequence.resources.data.ec2 Instance.instanceType
service.detection.sequence.resources.data.ec2 Instance.outpostArn
service.detection.sequence.resources.data.ec2 Instance.platform
service.detection.sequence.resources.data.ec2 Instance.productCodes.productCodeId
service.detection.sequence.resources.data.ec2 Instance.productCodes.productCodeType

Nome do campo JSON
service.detection.sequence.resources.data.ec2 LaunchTemplate.ec2InstanceUids
service.detection.sequence.resources.data.ec2 LaunchTemplate.version
service.detection.sequence.resources.data.ec2 NetworkInterface.ipv6Addresses
service.detection.sequence.resources.data.ec2 NetworkInterface.privateIpAddresses.privateDnsName
service.detection.sequence.resources.data.ec2 NetworkInterface.privateIpAddresses.privateIpAddress
service.detection.sequence.resources.data.ec2 NetworkInterface.publicIp
service.detection.sequence.resources.data.ec2 NetworkInterface.securityGroups.groupId
service.detection.sequence.resources.data.ec2 NetworkInterface.securityGroups.groupName
service.detection.sequence.resources.data.ec2 NetworkInterface.subNetId
service.detection.sequence.resources.data.ec2 NetworkInterface.vpcId
service.detection.sequence.resources.data.ec2 Vpc.ec2InstanceUids
service.detection.sequence.resources.data.ecs Cluster.ec2InstanceUids
service.detection.sequence.resources.data.ecs Cluster.status
service.detection.sequence.resources.data.ecs Task.containerUids
service.detection.sequence.resources.data.ecs Task.createdAt
service.detection.sequence.resources.data.ecs Task.launchType
service.detection.sequence.resources.data.ecs Task.taskDefinitionArn
service.detection.sequence.resources.data.eks Cluster.arn
service.detection.sequence.resources.data.eks Cluster.createdAt

Nome do campo JSON
service.detection.sequence.resources.data.eks Cluster.ec2InstanceUids
service.detection.sequence.resources.data.eks Cluster.status
service.detection.sequence.resources.data.eks Cluster.vpcId
service.detection.sequence.resources.data.iam InstanceProfile.ec2InstanceUids
service.detection.sequence.resources.data.iam InstanceProfile.id
service.detection.sequence.resources.data.kubernetes Workload.containerUids
service.detection.sequence.resources.data.kubernetes Workload.namespace
service.detection.sequence.resources.data.kubernetes Workload.type
service.detection.sequence.resources.data.s3 Bucket.accountPublicAccess.publicAclAccess
service.detection.sequence.resources.data.s3 Bucket.accountPublicAccess.publicAclIgnoreBehavior
service.detection.sequence.resources.data.s3 Bucket.accountPublicAccess.publicBucketRestrictBehavior
service.detection.sequence.resources.data.s3 Bucket.accountPublicAccess.publicPolicyAccess
service.detection.sequence.resources.data.s3 Bucket.bucketPublicAccess.publicAclAccess
service.detection.sequence.resources.data.s3 Bucket.bucketPublicAccess.publicAclIgnoreBehavior
service.detection.sequence.resources.data.s3 Bucket.bucketPublicAccess.publicBucketRestrictBehavior
service.detection.sequence.resources.data.s3 Bucket.bucketPublicAccess.publicPolicyAccess
service.detection.sequence.resources.data.s3 Bucket.createdAt
service.detection.sequence.resources.data.s3 Bucket.effectivePermission

Nome do campo JSON
service.detection.sequence.resources.data.s3 Bucket.encryptionKeyArn
service.detection.sequence.resources.data.s3 Bucket.encryptionType
service.detection.sequence.resources.data.s3 Bucket.ownerId
service.detection.sequence.resources.data.s3 Bucket.publicReadAccess
service.detection.sequence.resources.data.s3 Bucket.publicWriteAccess
service.detection.sequence.resources.data.s3 Bucket.s3ObjectUids
service.detection.sequence.resources.data.s3 Object.eTag
service.detection.sequence.resources.data.s3 Object.key
service.detection.sequence.resources.data.s3 Object.versionId
service.detection.sequence.resources.name
service.detection.sequence.resources.region
service.detection.sequence.resources.resourceType
service.detection.sequence.resources.service
service.detection.sequence.resources.tags.key
service.detection.sequence.resources.tags.value
service.detection.sequence.resources.uid
service.detection.sequence.sequence Indicators.key
service.detection.sequence.sequence Indicators.title
service.detection.sequence.sequence Indicators.values
service.detection.sequence.signals.ActorIds

Nome do campo JSON
service.detection.sequence.signals.count
service.detection.sequence.signals.criado em
service.detection.sequence.signals.description
service.detection.sequence.signals.endpointIDs
service.detection.sequence.signals.first SeenAt
service.detection.sequence.signals.last SeenAt
service.detection.sequence.signals.name
service.detection.sequence.signals.resourceUIDs
service.detection.sequence.signals.severity
service.detection.sequence.signals.signal Indicators.key
service.detection.sequence.signals.signal Indicators.title
service.detection.sequence.signals.signal Indicators.values
service.detection.sequence.signals.type
service.detection.sequence.signals.uid
service.detection.sequence.signals.Atualizado em
service.detection.sequence.uid
Service.DetectorID
service.ebs VolumeScanDetails.scanCompletedAt
service.ebs VolumeScanDetails.scanDetections.highestSeverityThreatDetails.count
service.ebs VolumeScanDetails.scanDetections.highestSeverityThreatDetails.severity

Nome do campo JSON
service.ebs VolumeScanDetails.scanDetections.highestSeverityThreatDetails.threatName
service.ebs VolumeScanDetails.scanDetections.scannedItemCount.files
service.ebs VolumeScanDetails.scanDetections.scannedItemCount.totalGb
service.ebs VolumeScanDetails.scanDetections.scannedItemCount.volumes
service.ebs VolumeScanDetails.scanDetections.threatDetectedByName.itemCount
service.ebs VolumeScanDetails.scanDetections.threatDetectedByName.shortened
service.ebs VolumeScanDetails.scanDetections.threatDetectedByName.threatNames.filePaths.fileName
service.ebs VolumeScanDetails.scanDetections.threatDetectedByName.threatNames.filePaths.filePath
service.ebs VolumeScanDetails.scanDetections.threatDetectedByName.threatNames.filePaths.volumeArn
service.ebs VolumeScanDetails.scanDetections.threatDetectedByName.threatNames.itemCount
service.ebs VolumeScanDetails.scanDetections.threatDetectedByName.uniqueThreatNameCount
service.ebs VolumeScanDetails.scanDetections.threatsDetectedItemCount.files
service.ebs VolumeScanDetails.scanStartedAt
service.ebs VolumeScanDetails.scanType
service.ebs VolumeScanDetails.sources
serviço.evento FirstSeen
serviço.evento LastSeen
serviço.malware ScanDetails.scanCategory
serviço.malware ScanDetails.scanConfiguration.incrementalScanDetails.baselineResourceArn

Nome do campo JSON
serviço.malware ScanDetails.scanConfiguration.triggerType
serviço.malware ScanDetails.threats.count
serviço.malware ScanDetails.threats.hash
serviço.malware ScanDetails.threats.itemDetails.additionalInfo.deviceName
serviço.malware ScanDetails.threats.itemDetails.additionalInfo.versionId
serviço.malware ScanDetails.threats.itemDetails.hash
serviço.malware ScanDetails.threats.itemDetails.itemPath
serviço.malware ScanDetails.threats.itemDetails.resourceArn
serviço.malware ScanDetails.threats.itemPaths.hash
serviço.malware ScanDetails.threats.itemPaths.nestedItemPath
serviço.malware ScanDetails.threats.source
serviço.malware ScanDetails.uniqueThreatCount
service.runtime Details.context.addressFamily
service.runtime Details.context.commandLineExample
service.runtime Details.context.fileSystemType
service.runtime Details.context.flags
service.runtime Details.context.ianaProtocolNumber
service.runtime Details.context.ldPreloadValue
service.runtime Details.context.libraryPath
service.runtime Details.context.memoryRegions

Nome do campo JSON
service.runtime Details.context.modifiedAt
service.runtime Details.context.modifyingProcess.euid
service.runtime Details.context.modifyingProcess.executablePath
service.runtime Details.context.modifyingProcess.executableSha256
service.runtime Details.context.modifyingProcess.lineage.euid
service.runtime Details.context.modifyingProcess.lineage.executablePath
service.runtime Details.context.modifyingProcess.lineage.name
service.runtime Details.context.modifyingProcess.lineage.namespacePid
service.runtime Details.context.modifyingProcess.lineage.parentUuid
service.runtime Details.context.modifyingProcess.lineage.pid
service.runtime Details.context.modifyingProcess.lineage.startTime
service.runtime Details.context.modifyingProcess.lineage.userId
service.runtime Details.context.modifyingProcess.lineage.uuid
service.runtime Details.context.modifyingProcess.name
service.runtime Details.context.modifyingProcess.namespacePid
service.runtime Details.context.modifyingProcess.parentUuid
service.runtime Details.context.modifyingProcess.pid
service.runtime Details.context.modifyingProcess.pwd
service.runtime Details.context.modifyingProcess.startTime
service.runtime Details.context.modifyingProcess.user

Nome do campo JSON
service.runtime Details.context.modifyingProcess.userId
service.runtime Details.context.modifyingProcess.uuid
service.runtime Details.context.mountSource
service.runtime Details.context.mountTarget
service.runtime Details.context.relatedFilePaths
service.runtime Details.context.releaseAgentPath
service.runtime Details.context.runcBinaryPath
service.runtime Details.context.scriptPath
service.runtime Details.context.serviceName
service.runtime Details.context.shellHistoryFilePath
service.runtime Details.context.socketPath
service.runtime Details.context.targetProcess.euid
service.runtime Details.context.targetProcess.executablePath
service.runtime Details.context.targetProcess.executableSha256
service.runtime Details.context.targetProcess.lineage.euid
service.runtime Details.context.targetProcess.lineage.executablePath
service.runtime Details.context.targetProcess.lineage.name
service.runtime Details.context.targetProcess.lineage.namespacePid
service.runtime Details.context.targetProcess.lineage.parentUuid
service.runtime Details.context.targetProcess.lineage.pid

Nome do campo JSON
service.runtime Details.context.targetProcess.lineage.startTime
service.runtime Details.context.targetProcess.lineage.userId
service.runtime Details.context.targetProcess.lineage.uuid
service.runtime Details.context.targetProcess.name
service.runtime Details.context.targetProcess.namespacePid
service.runtime Details.context.targetProcess.parentUuid
service.runtime Details.context.targetProcess.pid
service.runtime Details.context.targetProcess.pwd
service.runtime Details.context.targetProcess.startTime
service.runtime Details.context.targetProcess.user
service.runtime Details.context.targetProcess.userId
service.runtime Details.context.targetProcess.uuid
service.runtime Details.context.threatFilePath
service.runtime Details.context.toolCategory
service.runtime Details.context.toolName
service.runtime Details.process.euid
service.runtime Details.process.lineage.euid
service.runtime Details.process.lineage.executablePath
service.runtime Details.process.lineage.name
service.runtime Details.process.lineage.namespacePid

Nome do campo JSON
service.runtime Details.process.lineage.parentUuid
service.runtime Details.process.lineage.pid
service.runtime Details.process.lineage.startTime
service.runtime Details.process.lineage.userId
service.runtime Details.process.lineage.uuid
service.runtime Details.process.namespacePid
service.runtime Details.process.parentUuid
service.runtime Details.process.pid
service.runtime Details.process.pwd
service.runtime Details.process.startTime
service.runtime Details.process.user
service.runtime Details.process.userId
service.runtime Details.process.uuid
Serviço. Feedback do usuário

Regras de supressão em GuardDuty

Uma regra de supressão é um conjunto de critérios, que consistem em um atributo de filtro pareado com um valor, usados para filtrar descobertas arquivando automaticamente novas descobertas que correspondam aos critérios especificados. As regras de supressão podem ser usadas para filtrar descobertas de baixo valor, descobertas de falsos positivos ou ameaças nas quais você não pretende agir, para facilitar o reconhecimento das ameaças à segurança com maior impacto no ambiente.

Depois de criar uma regra de supressão, novas descobertas que correspondem aos critérios definidos na regra serão arquivadas automaticamente, desde que a regra de supressão esteja em vigor. É possível usar um filtro existente para criar uma regra de supressão ou definir um novo filtro para a regra de supressão ao criá-la. É possível configurar regras de supressão para suprimir tipos de descoberta inteiros ou definir critérios de filtro mais granulares para suprimir somente instâncias específicas de um determinado tipo de descoberta. As regras de supressão podem ser editadas a qualquer momento.

As descobertas suprimidas não são enviadas para AWS Security Hub CSPM o Amazon Simple Storage Service, Amazon Detective ou Amazon EventBridge, reduzindo o nível de ruído de descoberta se você consumir GuardDuty descobertas por meio do Security Hub CSPM, de um SIEM de terceiros ou de outros aplicativos de alerta e emissão de tíquetes. Se você tiver ativadoProteção contra malware para o EC2, as GuardDuty descobertas suprimidas não iniciarão uma verificação de malware.

GuardDuty continua gerando descobertas mesmo quando elas correspondem às suas regras de supressão; no entanto, essas descobertas são automaticamente marcadas como arquivadas. A descoberta arquivada é armazenada GuardDuty por 90 dias e pode ser visualizada a qualquer momento durante esse período. Você pode ver as descobertas suprimidas no GuardDuty console selecionando Arquivado na tabela de descobertas ou por meio da GuardDuty API usando a ListFindings API com um `findingCriteria` critério de `service.archived` igual a verdadeiro.

> **Note**
>
> Em um ambiente com várias contas, somente o GuardDuty administrador pode criar regras de supressão.

Usando regras de supressão com a Detecção de Ameaças Avançada

GuardDuty A Detecção Estendida de Ameaças detecta automaticamente ataques em vários estágios que abrangem fontes de dados, vários tipos de AWS recursos e tempo, em um. Conta da AWS Ela correlaciona eventos em diferentes fontes de dados para identificar cenários que se apresentam como uma ameaça potencial ao seu ambiente da AWS e, em seguida, gera uma descoberta de sequência de ataque. Para obter mais informações, consulte Como funciona a Detecção de Ameaças Avançada.

Quando você cria regras de supressão que arquivam descobertas, a Detecção de Ameaças Avançada não pode usar essas descobertas arquivadas ao correlacionar eventos para sequências

de ataque. Regras amplas de supressão podem afetar a capacidade de detectar comportamentos alinhados com GuardDuty a detecção de ataques em vários estágios. As descobertas arquivadas devido às regras de supressão não são consideradas sinais para sequências de ataque. Por exemplo, se você criar uma regra de supressão que arquive todas as descobertas relacionadas ao cluster EKS em vez de ter como alvo atividades conhecidas específicas, GuardDuty não conseguirá usar essas descobertas para detectar uma sequência de ataque em que um agente de ameaças explora um contêiner, obtém tokens privilegiados e acessa recursos confidenciais.

Considere as seguintes recomendações de GuardDuty:

- Continue usando as regras de supressão para reduzir os alertas de atividades confiáveis conhecidas.
- Mantenha as regras de supressão focadas em comportamentos específicos para os quais você não GuardDuty deseja gerar uma descoberta.

Casos de uso comuns para regras de supressão e exemplos

Veja a seguir os tipos de descoberta em casos de uso comuns para aplicar regras de supressão: Escolha o nome da descoberta para aprender mais sobre a descoberta. Revise a descrição do caso de uso para decidir se deseja criar uma regra de supressão para esse tipo de descoberta.

> **Important**
>
> GuardDuty recomenda que você crie regras de supressão de forma reativa e somente para descobertas para as quais você identificou repetidamente falsos positivos em seu ambiente.

- UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS: use uma regra de supressão para arquivar automaticamente as descobertas geradas quando a rede da VPC é configurada para rotear o tráfego da Internet de modo que ele saia de um gateway on-premises, e não de um gateway da Internet da VPC.

  Essa descoberta é gerada quando a rede é configurada para rotear o tráfego da Internet de modo que ele saia de um gateway on-premises e não de um gateway da Internet (IGW) da VPC. Configurações comuns, como usar AWS Outposts, ou conexões de VPN da VPC podem resultar em tráfego roteado dessa maneira. Se esse comportamento for esperado, é recomendável usar regras de supressão no e criar uma regra que consiste em dois critérios de filtro. O primeiro critério é tipo de descoberta, que deve ser `UnauthorizedAccess:IAMUser/`

`InstanceCredentialExfiltration.OutsideAWS`. O segundo critério de filtro é o endereço IPv4 do chamador de API com o endereço IP ou intervalo CIDR do seu gateway da Internet on-premises. O exemplo abaixo representa o filtro que você usaria para suprimir esse tipo de descoberta com base no endereço IP do chamador da API.

```
Finding type: UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS
 API caller IPv4 address: 198.51.100.6
```

> **Note**
>
> Para incluir vários IPs de chamadores de API, você pode adicionar cada endereço IP à lista de valores para Iguais ou NotEquals condições, ou usar padrões curinga para correspondências ou condições. NotMatches Um NotEquals valor igual a ou igual também pode ser um intervalo CIDR, que corresponde a qualquer endereço IP dentro desse intervalo.

- Recon:EC2/Portscan: use uma regra de supressão para arquivar automaticamente as descobertas ao usar um aplicativo de avaliação de vulnerabilidade.

  A regra de supressão deve consistir em dois critérios de filtro. O primeiro critério deve usar o atributo Tipo de descoberta com um valor de `Recon:EC2/Portscan`. O segundo critério de filtro deve corresponder a uma ou mais instâncias que hospedam essas ferramentas de avaliação de vulnerabilidade. É possível usar o atributo ID da imagem da instância ou o atributo de valor da Tag dependendo de quais critérios forem identificáveis com as instâncias que hospedam essas ferramentas. O exemplo abaixo representa o filtro que você usaria para suprimir esse tipo de descoberta com base em instâncias com uma determinada AMI.

  ```
  Finding type: Recon:EC2/Portscan Instance image ID: ami-999999999
  ```

- UnauthorizedAccess:EC2/SSHBruteForce: use uma regra de supressão para arquivar automaticamente as descobertas quando elas forem direcionadas a instâncias bastion.

  Se o alvo da tentativa de força bruta for um bastião hospedeiro, isso pode representar o comportamento esperado para seu AWS ambiente. Se for esse o caso, recomendamos configurar uma regra de supressão para essa descoberta. A regra de supressão deve consistir em dois critérios de filtro. O primeiro critério deve usar o atributo Tipo de descoberta com um valor de `UnauthorizedAccess:EC2/SSHBruteForce`. O segundo critério de filtro deve corresponder a uma ou mais instâncias que servem como um bastion host. É possível usar o atributo ID

da imagem da instância ou o atributo de valor da Tag dependendo de quais critérios forem identificáveis com as instâncias que hospedam essas ferramentas. O exemplo abaixo representa o filtro que você usaria para suprimir esse tipo de descoberta com base em instâncias com um determinado valor de tag de instância.

```
Finding type: UnauthorizedAccess:EC2/SSHBruteForce Instance tag value: devops
```

- Recon:EC2/PortProbeUnprotectedPort: use uma regra de supressão para arquivar automaticamente as descobertas quando forem elas direcionadas a instâncias intencionalmente expostas.

  Pode haver casos em que as instâncias são intencionalmente expostas; por exemplo, se estiverem hospedando servidores web. Se esse for o caso em seu AWS ambiente, recomendamos que você configure uma regra de supressão para essa descoberta. A regra de supressão deve consistir em dois critérios de filtro. O primeiro critério deve usar o atributo Tipo de descoberta com um valor de `Recon:EC2/PortProbeUnprotectedPort`. O segundo critério de filtro deve corresponder a uma ou mais instâncias que servem como um bastion host. É possível usar o atributo ID da imagem da instância ou o atributo de valor da Tag dependendo de quais critérios forem identificáveis com as instâncias que hospedam essas ferramentas. O exemplo abaixo representa o filtro que você usaria para suprimir esse tipo de descoberta com base em instâncias com uma determinada chave de tag de instância no console.

  ```
  Finding type: Recon:EC2/PortProbeUnprotectedPort Instance tag key: prod
  ```

Regras de supressão recomendadas para descobertas do Monitoramento de runtime.

- O PrivilegeEscalation:Runtime/DockerSocketAccessed é gerado quando um processo dentro de um contêiner se comunica com o soquete do Docker. Pode haver contêineres em seu ambiente que precisem acessar o soquete do Docker por motivos legítimos. O acesso a partir desses contêineres gerará a descoberta PrivilegeEscalation:Runtime/DockerSocketAccessed. Se esse for um caso em seu AWS ambiente, recomendamos que você configure uma regra de supressão para esse tipo de descoberta. O primeiro critério deve usar o campo Tipo de descoberta com um valor igual a `PrivilegeEscalation:Runtime/DockerSocketAccessed`. O segundo critério de filtro é o campo Caminho executável com valor igual ao do processo `executablePath` na descoberta gerada. Como alternativa, o segundo critério de filtro pode usar o SHA-256 campo Executável com valor igual ao do processo `executableSha256` na descoberta gerada.

- Os clusters do Kubernetes executam seus próprios servidores DNS como pods, como `coredns`. Portanto, para cada consulta de DNS de um pod, GuardDuty captura dois eventos de DNS — um do pod e outro do pod do servidor. Isso pode gerar duplicatas para as seguintes descobertas de DNS:
  - Backdoor:Runtime/C&CActivity.B! DNS
  - CryptoCurrency:Runtime/BitcoinTool.B! DNS
  - Impact:Runtime/AbusedDomainRequest.Reputation
  - Impact:Runtime/BitcoinDomainRequest.Reputation
  - Impact:Runtime/MaliciousDomainRequest.Reputation
  - Impact:Runtime/SuspiciousDomainRequest.Reputation
  - Trojan:Runtime/BlackholeTraffic! DNS
  - Trojan:Runtime/DGADomainRequest.C! DNS
  - Trojan:Runtime/DriveBySourceTraffic! DNS
  - Trojan:Runtime/DropPoint! DNS
  - Trojan:Runtime/PhishingDomainRequest! DNS

  As descobertas duplicadas incluirão detalhes do pod, do contêiner e do processo que correspondem ao pod do seu servidor DNS. Você pode configurar uma regra de supressão para suprimir essas descobertas duplicadas usando esses campos. O primeiro critério de filtro deve usar o campo Tipo de descoberta com valor igual a um tipo de descoberta de DNS da lista de descobertas fornecida anteriormente nesta seção. O segundo critério de filtro pode ser Caminho executável com valor igual ao do seu servidor DNS `executablePath` ou Executável SHA-256 com valor igual ao do seu servidor DNS `executableSHA256` na descoberta gerada. Como terceiro critério de filtro opcional, é possível usar o campo de imagem de contêiner do Kubernetes com valor igual à imagem de contêiner do seu pod de servidor DNS na descoberta gerada.

Criação de regras de supressão em GuardDuty

Uma regra de supressão é um conjunto de critérios que inclui o uso de atributos de filtro e o fornecimento de valores para os quais você não GuardDuty deseja gerar um tipo de descoberta. Os tipos de descoberta que correspondem a esses critérios são arquivados automaticamente. Para reduzir o ruído, as descobertas suprimidas não são enviadas para nenhum dos Serviços da AWS quais você possa se integrar. Para obter mais informações sobre como criar regras de supressão, consulte Regras de supressão.

Você pode visualizar, criar e gerenciar regras de supressão usando a página Regras de supressão no console. GuardDuty As regras de supressão também podem ser geradas a partir dos filtros salvos existentes. Para obter mais informações sobre a criação de filtros, consulte Filtrando descobertas em GuardDuty.

Os critérios do filtro podem incluir uma correspondência exata usando iguais e NotEquals operadores, uma correspondência curinga usando os operadores Correspondências e, ou correspondência de comparação usando NotMatches operadores GreaterThan GreaterThanEquals, e. LessThan LessThanEquals Mais informações sobre os operadores disponíveis podem ser encontradas na Conditions página.

Escolha seu método de acesso preferido para criar uma regra de supressão para GuardDuty encontrar tipos.

Console

Como criar uma regra de supressão usando o console:

1. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.
2. Na página Regras de supressão, clique em Criar regra de supressão para abrir o formulário Criar regra de supressão.
3. Insira um nome para a regra de supressão. O nome deve ter de 3 a 64 caracteres. Os caracteres válidos são a-z A-Z, 0-9, ponto (.), hífen (-) e sublinhado (_).
4. A descrição é opcional. Se você inserir uma descrição, ela pode ter até 512 caracteres. Os caracteres válidos são a-z A-Z, 0-9, ponto (.), hífen (-), dois pontos (:), colchetes ({} () []), barra (/) e espaço.
5. A classificação é opcional. Pode ser um valor numérico de 1 até a contagem total de filtros e regras de supressão, mais 1.
6. Na seção Atributos, selecione uma chave e um operador no menu suspenso.
7. Insira o valor “string” ou “date” do datepicker com base na chave selecionada. Se for um valor de string, digite o texto e pressione enter. Vários valores podem ser adicionados no caso de valores de string.
8. Critérios adicionais podem ser adicionados selecionando Adicionar critérios para adicionar outro conjunto de chave, operador e valor (es).
9. Selecione Criar regra de supressão para criar e salvar a regra de supressão.

Também é possível criar uma regra de supressão a partir de um filtro já salvo. Para obter mais informações sobre como criar ARNs, consulte Filtrando descobertas em GuardDuty.

Para criar uma regra de supressão a partir de um filtro salvo:

1. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.
2. Na página Descobertas, no menu Regras salvas, selecione uma regra de conjunto de filtros salva. Isso exibirá automaticamente o conjunto de filtros e as descobertas que correspondem aos critérios.
3. Você também pode adicionar mais critérios de filtro a essa regra salva. Se você não precisar de critérios de filtro adicionais, pule esta etapa. Para adicionar um ou mais critérios de filtro, siga as etapas de 3 a 7 em Adding filters on Findings page e continue com as etapas a seguir.
4. Depois de adicionar os critérios de filtro e confirmar que as descobertas filtradas atendem aos seus requisitos, escolha Criar regra de supressão.
5. Insira um nome para a regra de supressão. O nome deve ter de 3 a 64 caracteres. Os caracteres válidos são a-z A-Z, 0-9, ponto (.), hífen (-) e sublinhado (_).
6. A descrição é opcional. Se você inserir uma descrição, ela pode ter até 512 caracteres.
7. Escolha Criar.
8. Se você não precisar adicionar outros critérios de filtro à regra salva, siga as etapas de 4 a 7 para criar o filtro.

API/CLI

Para criar uma regra de supressão usando a API:

1. Também é possível criar regras de supressão por meio da API CreateFilter. Para fazer isso, especifique os critérios de filtro em um arquivo JSON seguindo o formato do exemplo detalhado abaixo. O exemplo abaixo suprimirá qualquer descoberta não arquivada de baixa gravidade que tenha uma solicitação de DNS para o domínio `test.example.com`. Para descobertas de gravidade média, a lista de entrada será `["4", "5", "7"]`. Para descobertas de alta gravidade, a lista de entrada será `["6", "7", "8"]`. Para descobertas de gravidade crítica, a lista de entrada será `["9", "10"]`. Você também pode filtrar com base em qualquer valor na lista.

O exemplo a seguir adiciona um filtro para descobertas de baixa severidade para funções lambda com prefixo de nome de função "MyFunc" e tag de função com prefixo diferente de "" TestTag

```
{
    "Criterion": {
        "service.action.dnsRequestAction.domain": {
            "Equals": [
                "test.example.com"
            ]
        },
        "severity": {
            "Equals": [
                "1",
                "2",
                "3"
            ]
        }
    }
}
```

Você pode criar regras de supressão usando caracteres curingas* e? . Os curingas nos filtros são suportados usando somente correspondências e NotMatches operadores. Para corresponder a qualquer número de caracteres, você pode usar * no valor do atributo e, para corresponder a um único caractere, você pode usar? no valor do atributo. Os filtros suportam no máximo 5 atributos em uma única condição curinga e no máximo 5 caracteres curinga em um único atributo. O exemplo a seguir adiciona um filtro para o nome do Lambda que corresponde ao prefixo “MyFunc", mas não às funções do Lambda com tags com "TestTag" como prefixo seguido por 0 a 2 caracteres.

```
{
    "Criterion": {
        "resource.lambdaDetails.functionName": {
            "Matches": [
                "MyFunc*"
            ]
        },
```

```
        "resource.lambdaDetails.tags.key": {
            "NotMatches": [
                "TestTag??"
            ]
        }
    }
}
```

Para obter uma lista de nomes de campo JSON e seus equivalentes de console, consulte Filtros de propriedades em GuardDuty.

Para testar seus critérios de filtro, use o mesmo critério JSON na API ListFindings e confirme se as descobertas corretas foram selecionadas. Para testar seus critérios de filtro usando, AWS CLI siga o exemplo usando seu próprio detectorID e arquivo.json.

Para encontrar o da `detectorId` sua conta e da região atual, consulte a página Configurações no https://console.aws.amazon.com/guardduty/ console ou execute a ListDetectors API.

```
aws guardduty list-detector
```

```
aws guardduty list-findings \
--detector-id 12abc34d567e8fa901bc2d34e56789f0 \
--region us-east-1 \
--finding-criteria file://criteria.json
```

> **Note**
>
> A correspondência de curingas não está disponível para ListFindings e. GetFindingsStatistics Os critérios que contêm curingas não podem ser validados usando e. ListFindings GetFindingsStatistics

2. Carregue seu filtro para ser usado como regra de supressão com a API CreateFilter ou usando a AWS CLI seguindo o exemplo abaixo com seu próprio ID de detector, um nome para a regra de supressão e um arquivo .json.

Para encontrar o da `detectorId` sua conta e da região atual, consulte a página Configurações no https://console.aws.amazon.com/guardduty/ console ou execute a ListDetectors API.

```
aws guardduty create-filter \
--detector-id 12abc34d567e8fa901bc2d34e56789f0 \
--region us-east-1 \
--action ARCHIVE \
--name yourfiltername \
--finding-criteria file://criteria.json
```

Você pode ver uma lista de seus filtros programaticamente com a API ListFilter. Você pode ver os detalhes de um filtro individual fornecendo o nome do filtro à API GetFilter. Atualize os filtros usando UpdateFilter ou exclua-os com a API DeleteFilter.

Atualizando as regras de supressão no GuardDuty

Esta seção fornece as etapas para atualizar uma regra de supressão Conta da AWS em seu local específico Região da AWS.

Você pode atualizar as regras de supressão existentes na página Regras de supressão no GuardDuty console. GuardDuty suporta a atualização da descrição, classificação e critérios de filtro do filtro de supressão a partir do GuardDuty console ou usando o. GuardDuty CLI/API A atualização da regra de supressão segue as mesmas restrições nos valores de campo para descrição, classificação e critérios deCriar regras de supressão.

Caso tenha uma conta-membro, sua conta de administrador poderá realizar essa ação na sua conta. Para obter mais informações, consulte Relações entre administradores do Macie e contas de membros.

Escolha seu método de acesso preferido para excluir uma regra de supressão para GuardDuty encontrar tipos.

Console

1. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.

2. Na página Regras de supressão, selecione a regra de supressão a ser atualizada.
3. No menu suspenso Ações, selecione Atualizar regra de supressão.
4. Isso abre o formulário existente da regra de supressão.
5. Faça alterações na seção Descrição, Classificação e Atributos conforme necessário.
6. Selecione Atualizar regra de supressão para atualizar a regra de supressão.

API/CLI

Para atualizar uma regra de supressão usando a API:

1. Você pode atualizar as regras de supressão por meio da UpdateFilter API. Somente a descrição, a classificação e os critérios podem ser atualizados usando a UpdateFilter API. Todos esses três campos são opcionais.
2. Para atualizar um filtro existente, você precisará do nome do filtro que está planejando atualizar.
3. Se você quiser atualizar os critérios existentes, crie um arquivo JSON com os critérios atualizados da mesma forma que você criou o filtro pela primeira vez. Um exemplo de critério para suprimir qualquer descoberta não arquivada de baixa gravidade que tenha uma solicitação de DNS para o domínio test.example.com. Para descobertas de gravidade média, a lista de entrada será ["4", “5", “7"]. Para descobertas de alta gravidade, a lista de entrada será ["6", “7", “8"]. Para descobertas de gravidade crítica, a lista de entrada será ["9", “10"]. Você também pode filtrar com base em qualquer valor na lista. O exemplo a seguir adiciona um filtro para descobertas de baixa gravidade.

```
{
    "Criterion": {
        "service.action.dnsRequestAction.domain": {
            "Equals": [
                "test.example.com"
            ]
        },
        "severity": {
            "Equals": [
                "1",
                "2",
                "3"
            ]
```

```
        }
    }
}
```

Para obter uma lista de nomes de campo JSON e seus equivalentes de console, consulte Filtros de propriedades em GuardDuty.

Para testar seus critérios de filtro, use o mesmo critério JSON na API ListFindings e confirme se as descobertas corretas foram selecionadas. Para testar seus critérios de filtro usando, AWS CLI siga o exemplo usando seu próprio detectorID e arquivo.json.

Para encontrar o da `detectorId` sua conta e da região atual, consulte a página Configurações no https://console.aws.amazon.com/guardduty/ console ou execute a ListDetectors API.

```
aws guardduty list-detectors --region us-east-1
```

4. Se quiser atualizar a descrição, você pode incluir o parâmetro de descrição na chamada da CLI.
5. Se quiser atualizar a classificação, você pode incluir o parâmetro de classificação na chamada da CLI.
6. Se você quiser atualizar de um filtro de supressão para um filtro normal, use o parâmetro de ação e o valor como ARCHIVE na chamada da CLI.
7. Atualize sua API de filtro existente ou use o AWS CLI seguinte exemplo abaixo com seu próprio ID de detector, um nome para a regra de supressão e o arquivo.json.
8. Veja a seguir um exemplo de CLI que atualiza todos os parâmetros descritos acima. Você pode selecionar os parâmetros específicos a serem atualizados para seu caso de uso no comando -

```
aws guardduty update-filter \
--detector-id 12abc34d567e8fa901bc2d34e56789f0 \
--region us-east-1 \
--action ARCHIVE \
--rank 1 \
--description "Updated description" \
```

```
--finding-criteria file://criteria.json
```

Excluindo regras de supressão em GuardDuty

Esta seção fornece as etapas para excluir uma regra de supressão Conta da AWS em seu local específico Região da AWS.

Pode ser necessário excluir uma regra de supressão que não represente mais um comportamento esperado em seu ambiente. Você não deseja mais suprimir o tipo de descoberta associado para que isso GuardDuty possa gerar um tipo de descoberta.

Caso tenha uma conta-membro, sua conta de administrador poderá realizar essa ação na sua conta. Para obter mais informações, consulte Relações entre administradores do Macie e contas de membros.

Escolha seu método de acesso preferido para excluir uma regra de supressão para GuardDuty encontrar tipos.

Console

1. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.
2. Na página Regras de supressão, selecione a regra de supressão a ser excluída.
3. No menu suspenso Ações, selecione Excluir regra de supressão.
4. Ele exibe um pop-up de confirmação. Selecione Excluir para continuar com a exclusão. Ou selecione Cancelar para cancelar a operação.

API/CLI

Execute a API DeleteFilter. Especifique o nome do filtro e o ID do detector associado para a região específica.

Como alternativa, você pode usar o AWS CLI exemplo a seguir substituindo os valores formatados em: *red*

```
aws guardduty delete-filter \
--detector-id 12abc34d567e8fa901bc2d34e56789f0 \
--filter-name filterName \
--region us-east-1
```

Para encontrar o da `detectorId` sua conta e da região atual, consulte a página Configurações no https://console.aws.amazon.com/guardduty/ console ou execute a ListDetectors API.

Métricas da regra de supressão

Com a Amazon GuardDuty, você pode monitorar com que frequência cada regra de supressão corresponde e arquiva as descobertas. GuardDuty publica essas métricas na Amazon CloudWatch sob o AWS/GuardDuty namespace.

> **GuardDuty conta as descobertas correspondidas e as suprimidas de forma diferente**
>
> GuardDuty é emitido FindingsMatchedByFilter quando uma descoberta corresponde a uma regra de supressão ou a um filtro NOOP (um filtro sem ação). Essa métrica é incrementada independentemente da ação do filtro. GuardDuty é emitida FindingsSuppressedByFilter somente quando a ação da regra é Arquivar e a regra é a regra de arquivamento de maior prioridade para essa descoberta.

GuardDuty publica métricas de regras de supressão com base na configuração da sua conta:

- Para contas autônomas (que não fazem parte de uma organização), GuardDuty publica métricas nessa conta.
- Para contas que fazem parte de uma organização, GuardDuty publica métricas na conta do GuardDuty administrador delegado. Para obter mais informações sobre como as contas de administrador e membro funcionam em GuardDuty, consulteGerenciando várias contas na Amazon GuardDuty.

Detalhes métricos

A tabela a seguir descreve as CloudWatch métricas da Amazon GuardDuty publicadas para regras de supressão.

Métrica	Unidade	Description
`FindingsMatchedByFilter`	Contagem	O número de descobertas que corresponderam aos critérios de uma regra de supressão ou filtro NOOP. Uma descoberta pode corresponder a várias regras de supressão ou filtros NOOP e GuardDuty contá-la uma vez por partida. Cada partida gera 1 ponto de dados.
`FindingsSuppressedByFilter`	Contagem	O número de descobertas arquivadas por uma regra de supressão. Quando várias regras correspondem à mesma descoberta, GuardDuty conta somente a regra com o menor `Rank` valor. Cada supressão gera 1 ponto de dados.

Veja métricas de regras de supressão na Amazon CloudWatch

Você pode encontrar métricas de regras de supressão no CloudWatch console da Amazon sob o AWS/GuardDutynamespace, agrupadas pela dimensão. FilterName O valor da `FilterName` dimensão é o nome da regra ou filtro de supressão. Para obter instruções sobre como localizar e representar graficamente métricas na Amazon CloudWatch, consulte Visualizar métricas disponíveis no Guia CloudWatch do usuário da Amazon.

Customizing threat detection with entity lists and IP address lists

A Amazon GuardDuty monitora a segurança do seu AWS ambiente analisando e processando registros de fluxo de VPC, registros de AWS CloudTrail eventos e registros de DNS. Ao habilitar um ou mais planos de GuardDuty proteção Use-case focados (exceto Monitoramento de runtime), você pode expandir os recursos de monitoramento internos GuardDuty.

Com listas, GuardDuty ajuda você a personalizar o escopo da detecção de ameaças em seu ambiente. Você pode configurar GuardDuty para parar de gerar descobertas de suas fontes confiáveis e gerar descobertas de fontes maliciosas conhecidas a partir de suas listas de ameaças. GuardDuty continua oferecendo suporte a listas de endereços IP antigas e estende o suporte a listas de entidades (recomendadas) que podem conter endereços IP, domínios ou ambos.

Tópicos

- Noções básicas sobre listas de entidades e listas de endereços IP
- Considerações importantes sobre listas GuardDuty
- Formatos das listas
- Noções básicas sobre os status de listas
- Configuração de pré-requisitos para listas de entidades e listas de endereços IP
- Como adicionar e ativar uma lista de entidades ou lista de IPs
- Atualizando uma lista de entidades ou lista de endereços IP
- De-activating lista de entidades ou lista de endereços IP
- Excluindo lista de entidades ou lista de endereços IP

Noções básicas sobre listas de entidades e listas de endereços IP

GuardDuty oferece duas abordagens de implementação: listas de entidades (recomendadas) e listas de IP. Ambas as abordagens ajudam você a especificar fontes confiáveis, que GuardDuty impedem de gerar descobertas, e ameaças conhecidas, que são GuardDuty usadas para gerar descobertas.

As listas de entidades oferecem suporte a endereços IP, nomes de domínio e hashes de SHA-256 arquivos. Elas usam acesso direto ao Amazon Simple Storage Service (Amazon S3) com uma única permissão do IAM que não afeta os limites de tamanho da política do IAM em várias regiões.

As listas de IP oferecem suporte somente para endereços IP e usam GuardDuty função vinculada a serviços (SLR) (SLR), exigindo atualizações da política do IAM por região, o que pode afetar os limites de tamanho da política do IAM.

As listas confiáveis (listas de entidades e listas de endereços IP) incluem entradas nas quais você confia para comunicação segura com sua AWS infraestrutura. GuardDuty não gera descobertas para entradas listadas em fontes confiáveis. A qualquer momento, você pode adicionar somente uma lista de entidades confiáveis e uma lista de endereços IP confiáveis Conta da AWS por região.

As listas de ameaças (listas de entidades e listas de endereços IP) incluem entradas que você identificou como fontes conhecidas maliciosas. Quando GuardDuty detecta uma atividade envolvendo essas fontes, ela gera descobertas para alertá-lo sobre possíveis problemas de segurança. Você pode criar suas próprias listas de ameaças ou incorporar feeds de inteligência de ameaças de terceiros. Essa lista pode ser fornecida por inteligência de ameaças de terceiros ou criada especificamente para sua organização. Além de gerar descobertas devido a uma atividade potencialmente suspeita, GuardDuty também gera descobertas com base em uma atividade que envolve entradas de suas listas de ameaças. A qualquer momento, você pode fazer upload de até seis listas de entidades de ameaças e listas de endereços IP de ameaças Conta da AWS por região.

> **Note**
>
> Para migrar de listas de endereços IP para listas de entidades, siga Pré-requisitos para listas de entidades, adicione e ative a lista de entidades necessária. Depois disso, você pode optar por desativar ou excluir a lista de endereços IP correspondente.

Considerações importantes sobre listas GuardDuty

Antes de começar a trabalhar com listas, leia as considerações a seguir:

- As listas de endereços IPs e listas de ameaças são aplicáveis somente ao tráfego destinado para domínios e endereços IP roteáveis publicamente.
- Em uma lista de entidades, as entradas se aplicam às CloudTrail descobertas dos registros de consulta de DNS do VPC Flow Logs no Amazon VPC e do Route53 Resolver.

  Em uma lista de endereços IP, as entradas se aplicam aos CloudTrail registros de fluxo de VPC nas descobertas do Amazon VPC, mas não às descobertas dos registros de consulta de DNS do Route53 Resolver.
- Se você incluir o mesmo endereço IP ou domínio nas listas confiáveis e de ameaças, essa entrada na lista de confiáveis terá precedência. GuardDuty não gerará uma descoberta se houver uma atividade associada a essa entrada.
- Em um ambiente com várias contas, somente a conta GuardDuty do administrador pode gerenciar listas. Essa configuração se aplica automaticamente às contas dos membros. GuardDuty gera descobertas com base em uma atividade que envolve endereços IP (e domínios) maliciosos conhecidos das fontes de ameaça da conta do administrador e não gera descobertas com base em atividades que envolvem endereços IP (e domínios) das fontes confiáveis da conta do

administrador. Para obter mais informações, consulte Gerenciando várias contas na Amazon GuardDuty.

- Apenas os endereços IPv4 são aceitos. Os endereços IPv6 elásticos não são compatíveis.
- SHA-256 hashes de arquivos são suportados somente em listas de entidades de ameaças. Você não pode incluir hashes de arquivos em listas de entidades confiáveis ou listas de endereços IP.
- Depois de ativar, desativar ou excluir uma lista de entidades ou uma lista de endereços IP, estima-se que o processo seja concluído em 15 minutos. Em determinadas situações, o processo pode levar até 40 minutos para ser concluído.
- GuardDuty usa uma lista para detecção de ameaças somente quando o status da lista se torna Ativo.
- Sempre que você adiciona ou atualiza uma entrada no local do bucket do S3 da lista, você deve ativar a lista novamente. Para obter mais informações, consulte Atualizando uma lista de entidades ou lista de endereços IP.
- As listas de entidades e de endereços IP têm diferentes cotas. Para obter mais informações, consulte GuardDuty cotas.

Formatos das listas

GuardDuty aceita vários formatos de arquivo para suas listas e listas de entidades, com um máximo de 35 MB por arquivo. Cada formato tem requisitos e recursos específicos.

Texto sem formatação (TXT)

Esse formato oferece suporte a endereços IP, intervalos CIDR, nomes de domínio e hashes de SHA-256 arquivos. SHA-256 hashes de arquivos são suportados somente em listas de entidades de ameaças. Cada entrada deve aparecer em uma linha separada.

Example Exemplo de lista de entidades

```
192.0.2.1
192.0.2.0/24
example.com
example.org
*.example.org
```

Example Exemplo de lista de entidades de ameaça com hashes de arquivo

```
192.0.2.1
```

```
192.0.2.0/24
example.com
example.org
*.example.org
a665a45920422f9d417e4867efdc4fb8a04a1f3fff1fa07e998e86f7f7a27ae3
```

Example Exemplo de lista de endereços IP

```
192.0.2.0/24
198.51.100.1
203.0.113.1
```

Expressão estruturada de informações sobre ameaças (STIX)

Esse formato oferece suporte a endereços IP, blocos CIDR, nomes de domínio e hashes de SHA-256 arquivos. O STIX permite que você inclua contexto adicional com sua inteligência de ameaças. GuardDuty processa endereços IP, intervalos CIDR, nomes de domínio e hashes de SHA-256 arquivos dos indicadores STIX. SHA-256 hashes de arquivos são suportados somente em listas de entidades de ameaças.

Example Exemplo de uma lista de entidades

```
<?xml version="1.0" encoding="UTF-8"?>
<stix:STIX_Package
    xmlns:cyboxCommon="http://cybox.mitre.org/common-2"
    xmlns:cybox="http://cybox.mitre.org/cybox-2"
    xmlns:cyboxVocabs="http://cybox.mitre.org/default_vocabularies-2"
    xmlns:stix="http://stix.mitre.org/stix-1"
    xmlns:indicator="http://stix.mitre.org/Indicator-2"
    xmlns:stixCommon="http://stix.mitre.org/common-1"
    xmlns:stixVocabs="http://stix.mitre.org/default_vocabularies-1"
    xmlns:DomainNameObj="http://cybox.mitre.org/objects#DomainNameObject-1"
    id="example:Package-a1b2c3d4-1111-2222-3333-444455556666"
    version="1.2">
    <stix:Indicators>
        <stix:Indicator
            id="example:indicator-a1b2c3d4-aaaa-bbbb-cccc-ddddeeeeffff"
            timestamp="2025-08-12T00:00:00Z"
            xsi:type="indicator:IndicatorType"
            xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
            <indicator:Title>Malicious domain observed Example</indicator:Title>
```

```
            <indicator:Type xsi:type="stixVocabs:IndicatorTypeVocab-1.1">Domain
 Watchlist</indicator:Type>
            <indicator:Observable id="example:Observable-0000-1111-2222-3333">
                <cybox:Object id="example:Object-0000-1111-2222-3333">
                    <cybox:Properties xsi:type="DomainNameObj:DomainNameObjectType">
                        <DomainNameObj:Value condition="Equals">bad.example.com</
DomainNameObj:Value>
                    </cybox:Properties>
                </cybox:Object>
            </indicator:Observable>
        </stix:Indicator>
    </stix:Indicators>
</stix:STIX_Package>
```

Example Exemplo de lista de entidades de ameaça com hashes de arquivo

```
<?xml version="1.0" encoding="UTF-8"?>
<stix:STIX_Package
    xmlns:cyboxCommon="http://cybox.mitre.org/common-2"
    xmlns:cybox="http://cybox.mitre.org/cybox-2"
    xmlns:cyboxVocabs="http://cybox.mitre.org/default_vocabularies-2"
    xmlns:stix="http://stix.mitre.org/stix-1"
    xmlns:indicator="http://stix.mitre.org/Indicator-2"
    xmlns:stixCommon="http://stix.mitre.org/common-1"
    xmlns:stixVocabs="http://stix.mitre.org/default_vocabularies-1"
    xmlns:DomainNameObj="http://cybox.mitre.org/objects#DomainNameObject-1"
    xmlns:FileObj="http://cybox.mitre.org/objects#FileObject-2"
    id="example:Package-a1b2c3d4-1111-2222-3333-444455556666"
    version="1.2">
    <stix:Indicators>
        <stix:Indicator
            id="example:indicator-a1b2c3d4-aaaa-bbbb-cccc-ddddeeeeffff"
            timestamp="2025-08-12T00:00:00Z"
            xsi:type="indicator:IndicatorType"
            xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
            <indicator:Title>Malicious domain observed Example</indicator:Title>
            <indicator:Type xsi:type="stixVocabs:IndicatorTypeVocab-1.1">Domain
 Watchlist</indicator:Type>
            <indicator:Observable id="example:Observable-0000-1111-2222-3333">
                <cybox:Object id="example:Object-0000-1111-2222-3333">
                    <cybox:Properties xsi:type="DomainNameObj:DomainNameObjectType">
                        <DomainNameObj:Value condition="Equals">bad.example.com</
DomainNameObj:Value>
```

```
                    </cybox:Properties>
                </cybox:Object>
            </indicator:Observable>
        </stix:Indicator>
        <stix:Indicator
            id="example:indicator-a1b2c3d4-eeee-ffff-0000-111122223333"
            timestamp="2025-08-12T00:00:00Z"
            xsi:type="indicator:IndicatorType"
            xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
            <indicator:Title>File hash for malware variant</indicator:Title>
            <indicator:Type xsi:type="stixVocabs:IndicatorTypeVocab-1.1">File Hash
 Watchlist</indicator:Type>
            <indicator:Observable id="example:Observable-4444-5555-6666-7777">
                <cybox:Object id="example:File-4444-5555-6666-7777">
                    <cybox:Properties xsi:type="FileObj:FileObjectType">
                        <FileObj:Hashes>
                            <cyboxCommon:Hash>
                                <cyboxCommon:Type
 xsi:type="cyboxVocabs:HashNameVocab-1.0">SHA256</cyboxCommon:Type>
                                <cyboxCommon:Simple_Hash_Value
 condition="Equals">a665a45920422f9d417e4867efdc4fb8a04a1f3fff1fa07e998e86f7f7a27ae3</
cyboxCommon:Simple_Hash_Value>
                            </cyboxCommon:Hash>
                        </FileObj:Hashes>
                    </cybox:Properties>
                </cybox:Object>
            </indicator:Observable>
        </stix:Indicator>
    </stix:Indicators>
</stix:STIX_Package>
```

Example Exemplo de uma lista de endereços IP

```
<?xml version="1.0" encoding="UTF-8"?>
<stix:STIX_Package
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xmlns:stix="http://stix.mitre.org/stix-1"
    xmlns:stixCommon="http://stix.mitre.org/common-1"
    xmlns:ttp="http://stix.mitre.org/TTP-1"
    xmlns:cybox="http://cybox.mitre.org/cybox-2"
    xmlns:AddressObject="http://cybox.mitre.org/objects#AddressObject-2"
    xmlns:cyboxVocabs="http://cybox.mitre.org/default_vocabularies-2"
    xmlns:stixVocabs="http://stix.mitre.org/default_vocabularies-1"
```

```
    xmlns:example="http://example.com/"
    xsi:schemaLocation="
    http://stix.mitre.org/stix-1 http://stix.mitre.org/XMLSchema/core/1.2/
stix_core.xsd
    http://stix.mitre.org/Campaign-1 http://stix.mitre.org/XMLSchema/campaign/1.2/
campaign.xsd
    http://stix.mitre.org/Indicator-2 http://stix.mitre.org/XMLSchema/indicator/2.2/
indicator.xsd
    http://stix.mitre.org/TTP-2 http://stix.mitre.org/XMLSchema/ttp/1.2/ttp.xsd
    http://stix.mitre.org/default_vocabularies-1 http://stix.mitre.org/XMLSchema/
default_vocabularies/1.2.0/stix_default_vocabularies.xsd
    http://cybox.mitre.org/objects#AddressObject-2 http://cybox.mitre.org/XMLSchema/
objects/Address/2.1/Address_Object.xsd"
    id="example:STIXPackage-a78fc4e3-df94-42dd-a074-6de62babfe16"
    version="1.2">
    <stix:Observables cybox_major_version="1" cybox_minor_version="1">
        <cybox:Observable id="example:observable-80b26f43-
dc41-43ff-861d-19aff31e0236">
            <cybox:Object id="example:object-161a5438-1c26-4275-ba44-a35ba963c245">
                <cybox:Properties xsi:type="AddressObject:AddressObjectType"
 category="ipv4-addr">

 <AddressObject:Address_Valuecondition="InclusiveBetween">192.0.2.0##comma##192.0.2.255</
AddressObject:Address_Value>
                </cybox:Properties>
            </cybox:Object>
        </cybox:Observable>
        <cybox:Observable id="example:observable-b442b399-aea4-436f-bb34-
b9ef6c5ed8ab">
            <cybox:Object id="example:object-b422417f-bf78-4b34-ba2d-de4b09590a6d">
                <cybox:Properties xsi:type="AddressObject:AddressObjectType"
 category="ipv4-addr">
                    <AddressObject:Address_Value>198.51.100.1</
AddressObject:Address_Value>
                </cybox:Properties>
            </cybox:Object>
        </cybox:Observable>
        <cybox:Observable
 id="example:observable-1742fa06-8b5e-4449-9d89-6f9f32595784">
            <cybox:Object id="example:object-dc73b749-8a31-46be-803f-71df77565391">
                <cybox:Properties xsi:type="AddressObject:AddressObjectType"
 category="ipv4-addr">
                    <AddressObject:Address_Value>203.0.113.1</
AddressObject:Address_Value>
```

```
                </cybox:Properties>
            </cybox:Object>
        </cybox:Observable>
    </stix:Observables>
</stix:STIX_Package>
```

CSV Open Threat Exchange (OTX)[TM]

Esse formato suporta o bloco CIDR, endereços IP individuais, domínios e o tipo de SHA256 indicador para hashes de arquivos. SHA-256 hashes de arquivos são suportados somente em listas de entidades de ameaças. Esse formato de arquivo tem valores separados por vírgulas.

Example Exemplo de lista de entidades

```
Indicator type, Indicator, Description
CIDR, 192.0.2.0/24, example
IPv4, 198.51.100.1, example
IPv4, 203.0.113.1, example
Domain name, example.net, example
```

Example Exemplo de lista de entidades de ameaça com hashes de arquivo

```
Indicator type, Indicator, Description
CIDR, 192.0.2.0/24, example
IPv4, 198.51.100.1, example
IPv4, 203.0.113.1, example
Domain name, example.net, example
SHA256, a665a45920422f9d417e4867efdc4fb8a04a1f3fff1fa07e998e86f7f7a27ae3, example
```

Example Exemplo de lista de endereços IP

```
Indicator type, Indicator, Description
CIDR, 192.0.2.0/24, example
IPv4, 198.51.100.1, example
IPv4, 203.0.113.1, example
```

FireEyeCSV de inteligência de ameaças do [TM] iSight

Esse formato oferece suporte ao bloco CIDR, endereços IP individuais, domínios e hashes de SHA-256 arquivos na coluna. `sha256` SHA-256 hashes de arquivos são suportados somente

em listas de entidades de ameaças. Os exemplos de listas a seguir usam um formato CSV do FireEye™.

Example Exemplo de lista de entidades

```
reportId, title, threatScape, audience, intelligenceType, publishDate, reportLink,
 webLink, emailIdentifier, senderAddress, senderName, sourceDomain, sourceIp, subject,
 recipient, emailLanguage, fileName, fileSize, fuzzyHash, fileIdentifier, md5, sha1,
 sha256, description, fileType, packer, userAgent, registry, fileCompilationDateTime,
 filePath, asn, cidr, domain, domainTimeOfLookup, networkIdentifier, ip, port,
 protocol, registrantEmail, registrantName, networkType, url, malwareFamily,
 malwareFamilyId, actor, actorId, observationTime

01-00000001, Example, Test, Operational, threat, 1494944400,
 https://www.example.com/report/01-00000001, https://www.example.com/
report/01-00000001, , , , , , , , , , , , , , , , , , , , , , , , , , , , , 192.0.2.0/24, , ,
 Related, , , , , , network, , Ursnif, 21a14673-0d94-46d3-89ab-8281a0466099, , ,
 1494944400

01-00000002, Example, Test, Operational, threat, 1494944400,
 https://www.example.com/report/01-00000002, https://www.example.com/
report/01-00000002, , , , , , , , , , , , , , , , , , , , , , , , , , , , , , , , , , , , , , , Related,
 198.51.100.1, , , , , network, , Ursnif,
 12ab7bc4-62ed-49fa-99e3-14b92afc41bf, , ,1494944400

01-00000003, Example, Test, Operational, threat, 1494944400,
 https://www.example.com/report/01-00000003, https://www.example.com/
report/01-00000003, , , , , , , , , , , , , , , , , , , , , , , , , , , , , , , , , , , , , , , Related,
 203.0.113.1, , , , , network, , Ursnif, 8a78c3db-7bcb-40bc-a080-75bd35a2572d, , ,
 1494944400

 01-00000002, Malicious domain observed in test, Test, Operational, threat,
 1494944400, https://www.example.com/report/01-00000002,https://www.example.com/
report/01-00000002,,,,,,,,,,,,,,,,,,,,,,,,, 203.0.113.0/24, example.com,, Related,
 203.0.113.0, 8080, UDP,,, network,, Ursnif, fc13984c-c767-40c9-8329-f4c59557f73b,,,
 1494944400
```

Example Exemplo de lista de entidades de ameaça com hashes de arquivo

```
reportId, title, threatScape, audience, intelligenceType, publishDate, reportLink,
 webLink, emailIdentifier, senderAddress, senderName, sourceDomain, sourceIp, subject,
 recipient, emailLanguage, fileName, fileSize, fuzzyHash, fileIdentifier, md5, sha1,
 sha256, description, fileType, packer, userAgent, registry, fileCompilationDateTime,
```

```
 filePath, asn, cidr, domain, domainTimeOfLookup, networkIdentifier, ip, port,
 protocol, registrantEmail, registrantName, networkType, url, malwareFamily,
 malwareFamilyId, actor, actorId, observationTime

01-00000001, Example, Test, Operational, threat, 1494944400,
 https://www.example.com/report/01-00000001, https://www.example.com/
report/01-00000001, , , , , , , , , , , , , , , , , , , , , , , , , 192.0.2.0/24, , ,
 Related, , , , , , network, , Ursnif, 21a14673-0d94-46d3-89ab-8281a0466099, , ,
 1494944400

01-00000002, Example, Test, Operational, threat, 1494944400,
 https://www.example.com/report/01-00000002, https://www.example.com/
report/01-00000002, , , , , , , , , , , , , , , , , , , , , , , , , , , , , Related,
 198.51.100.1, , , , , network, , Ursnif,
 12ab7bc4-62ed-49fa-99e3-14b92afc41bf, , ,1494944400

01-00000003, Example, Test, Operational, threat, 1494944400,
 https://www.example.com/report/01-00000003, https://www.example.com/
report/01-00000003, , , , , , , , , , , , , , , , , , , , , , , , , , , , , Related,
 203.0.113.1, , , , , network, , Ursnif, 8a78c3db-7bcb-40bc-a080-75bd35a2572d, , ,
 1494944400

 01-00000002, Malicious domain observed in test, Test, Operational, threat,
 1494944400, https://www.example.com/report/01-00000002,https://www.example.com/
report/01-00000002,,,,,,,,,,,,,,,,,,,,,,, 203.0.113.0/24, example.com,, Related,
 203.0.113.0, 8080, UDP,,, network,, Ursnif, fc13984c-c767-40c9-8329-f4c59557f73b,,,
 1494944400

01-00000005, Malicious file hash, Test, Operational, threat,
 1494944400, https://www.example.com/report/01-00000005, https://
www.example.com/report/01-00000005, , , , , , , , , , , , , , , ,
 a665a45920422f9d417e4867efdc4fb8a04a1f3fff1fa07e998e86f7f7a27ae3, , , , , , , , , , , ,
 Related, , , , , , network, , Ursnif, 9b9a6ea0-3cbf-4e12-bd3e-0c1d7b4e5f6a, , ,
 1494944400
```

Example Exemplo de lista de endereços IP

```
reportId, title, threatScape, audience, intelligenceType, publishDate, reportLink,
 webLink, emailIdentifier, senderAddress, senderName, sourceDomain, sourceIp, subject,
 recipient, emailLanguage, fileName, fileSize, fuzzyHash, fileIdentifier, md5, sha1,
 sha256, description, fileType, packer, userAgent, registry, fileCompilationDateTime,
 filePath, asn, cidr, domain, domainTimeOfLookup, networkIdentifier, ip, port,
 protocol, registrantEmail, registrantName, networkType, url, malwareFamily,
 malwareFamilyId, actor, actorId, observationTime
```

```
01-00000001, Example, Test, Operational, threat, 1494944400,
 https://www.example.com/report/01-00000001, https://www.example.com/
report/01-00000001, , , , , , , , , , , , , , , , , , , , , , , , , 192.0.2.0/24, , ,
 Related, , , , , network, , Ursnif, 21a14673-0d94-46d3-89ab-8281a0466099, , ,
 1494944400

01-00000002, Example, Test, Operational, threat, 1494944400,
 https://www.example.com/report/01-00000002, https://www.example.com/
report/01-00000002, , , , , , , , , , , , , , , , , , , , , , , , , , , Related,
 198.51.100.1, , , , , network, , Ursnif,
 12ab7bc4-62ed-49fa-99e3-14b92afc41bf, , ,1494944400

01-00000003, Example, Test, Operational, threat, 1494944400,
 https://www.example.com/report/01-00000003, https://www.example.com/
report/01-00000003, , , , , , , , , , , , , , , , , , , , , , , , , , , Related,
 203.0.113.1, , , , , network, , Ursnif, 8a78c3db-7bcb-40bc-a080-75bd35a2572d, , ,
 1494944400
```

CSV Proofpoint™ ET Intelligence Feed

No formato ProofPoint CSV, você pode adicionar endereços IP ou nomes de domínio em uma única lista. A lista de exemplo a seguir usa o formato CSV `Proofpoint`. O fornecimento de um valor para o parâmetro `ports` é opcional. Se você não fornecer, deixe uma vírgula (,) no final.

Example Exemplo de lista de entidades

```
domain, category, score, first_seen, last_seen, ports (|)
198.51.100.1, 1, 100, 2000-01-01, 2000-01-01,
203.0.113.1, 1, 100, 2000-01-01, 2000-01-01, 80
```

Example Exemplo de lista de endereços IP

```
ip, category, score, first_seen, last_seen, ports (|)
198.51.100.1, 1, 100, 2000-01-01, 2000-01-01,
203.0.113.1, 1, 100, 2000-01-01, 2000-01-01, 80
```

AlienVaultFeed de reputação da TM

A lista de exemplos a seguir usa o formato `AlienVault`. Esse formato também suporta hashes de SHA-256 arquivo na coluna indicadora. SHA-256 hashes de arquivos são suportados somente em listas de entidades de ameaças.

Example Exemplo de lista de entidades

```
192.0.2.1#4#2#Malicious Host#KR##37.5111999512,126.974098206#3
192.0.2.2#4#2#Scanning Host#IN#Gurgaon#28.4666996002,77.0333023071#3
192.0.2.3#4#2##CN#Guangzhou#23.1166992188,113.25#3
www.test.org#4#2#Malicious Host#CA#Brossard#45.4673995972,-73.4832000732#3
www.example.com#4#2#Malicious Host#PL##52.2393989563,21.0361995697#3
```

Example Exemplo de lista de entidades de ameaça com hashes de arquivo

```
192.0.2.1#4#2#Malicious Host#KR##37.5111999512,126.974098206#3
192.0.2.2#4#2#Scanning Host#IN#Gurgaon#28.4666996002,77.0333023071#3
192.0.2.3#4#2##CN#Guangzhou#23.1166992188,113.25#3
www.test.org#4#2#Malicious Host#CA#Brossard#45.4673995972,-73.4832000732#3
www.example.com#4#2#Malicious Host#PL##52.2393989563,21.0361995697#3
a665a45920422f9d417e4867efdc4fb8a04a1f3fff1fa07e998e86f7f7a27ae3#4#2#Malicious
 Hash###0.0,0.0#3
```

Example Exemplo de lista de endereços IP

```
198.51.100.1#4#2#Malicious Host#US##0.0,0.0#3
203.0.113.1#4#2#Malicious Host#US##0.0,0.0#3
```

Noções básicas sobre os status de listas

Quando você adiciona uma lista de entidades ou uma lista de endereços IP, GuardDuty mostra o status dessa lista. A coluna Status indica se a lista é efetiva e se alguma ação é necessária. A lista a seguir descreve valores de status válidos:

- Ativo – indica que a lista está sendo usada atualmente para detecção personalizada de ameaças.
- Inativo – indica que a lista não está em uso no momento. GuardDuty Para usar essa lista para detecção de ameaças em seu ambiente, consulte Etapa 3: Ativando uma lista de entidades ou lista de endereços IP emComo adicionar e ativar uma lista de entidades ou lista de IPs.
- Erro – indica que há um problema com a lista. Passe o mouse sobre o status para ver os detalhes do erro.
- Ativando — Indica que GuardDuty iniciou o processo de ativação da lista. Você pode continuar monitorando o status dessa lista. Se não houver erro, o status deverá ser atualizado para Ativo. Enquanto o status permanecer Ativando, você não poderá realizar nenhuma ação nessa lista. Pode levar alguns minutos para que o status da lista mude para o estado Ativo.

- Desativação — Indica que GuardDuty iniciou o processo de desativação da lista. Você pode continuar monitorando o status dessa lista. Se não houver erro, o status deverá ser atualizado para Inativo. Enquanto o status permanecer Desativando, você não poderá realizar nenhuma ação nessa lista.
- Exclusão pendente – indica que a lista está em processo de ser excluída. Enquanto o status permanecer Exclusão pendente, você não poderá realizar nenhuma ação nessa lista.

Configuração de pré-requisitos para listas de entidades e listas de endereços IP

GuardDuty usa listas de entidades e listas de endereços IP para personalizar a detecção de ameaças em seu AWS ambiente. As listas de entidades (recomendadas) aceitam endereços IP e nomes de domínio, enquanto as listas de endereços IP aceitam apenas endereços IP. Antes de começar a criar essas listas, você deverá adicionar as permissões necessárias para o tipo de lista que deseja usar.

Pré-requisitos para listas de entidades

Quando você adiciona listas de entidades, GuardDuty lê suas listas confiáveis e de inteligência de ameaças dos buckets do S3. O perfil que você usa para criar listas de entidades deve ter a permissão `s3:GetObject` para que os buckets do S3 contenham essas listas.

> **Note**
>
> Em um ambiente com várias contas, somente a conta do GuardDuty administrador pode gerenciar listas, que se aplicam automaticamente às contas dos membros.

Se você ainda não tiver a `s3:GetObject` permissão para a localização do bucket do S3, use o exemplo de política a seguir e *`amzn-s3-demo-bucket`* substitua pela localização do bucket do S3.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
```

```
            "Effect": "Allow",
            "Action": "s3:GetObject",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/[object-key]"
        }
    ]
}
```

Pré-requisitos para listas de endereços IP

Várias identidades do IAM exigem permissões especiais para trabalhar com listas de IPs confiáveis e listas de ameaças. GuardDuty Uma identidade com a política gerenciada AmazonGuardDutyFullAccess_v2 (recomendado) anexada só pode renomear e desabilitar as listas de IP confiáveis e listas de ameaças carregadas.

Para conceder a várias identidades o acesso total para trabalhar com listas de IP confiáveis e listas de ameaças (além de renomear e desabilitar, isso inclui fazer upload, habilitar, excluir e atualizar a localização da lista), as seguintes ações devem estar presentes na política de permissões anexada a um usuário, um grupo ou uma função do IAM:

```
{
    "Effect": "Allow",
    "Action": [
        "iam:PutRolePolicy",
        "iam:DeleteRolePolicy"
    ],
    "Resource": "arn:aws:iam::555555555555:role/aws-service-role/
guardduty.amazonaws.com/AWSServiceRoleForAmazonGuardDuty"
}
```

> **Important**
>
> Essas ações não estão incluídas na política gerenciada `AmazonGuardDutyFullAccess`.

Usando SSE-KMS criptografia com listas de entidades e listas de IP

GuardDuty suportes SSE-AES256 e SSE-KMS criptografia para suas listas. SSE-C não é suportado. Para obter mais informações sobre os tipos de criptografia do S3, consulte Proteger dados usando criptografia do lado do servidor.

Independentemente de você usar listas de entidades ou listas de IP, se você usar SSE-KMS, adicione a seguinte declaração à sua AWS KMS key política. *123456789012*Substitua pelo seu próprio ID de conta.

```
{
    "Sid": "AllowGuardDutyServiceRole",
    "Effect": "Allow",
    "Principal": {
    "AWS": "arn:aws:iam::123456789012:role/aws-service-role/guardduty.amazonaws.com/
AWSServiceRoleForAmazonGuardDuty"
    },
    "Action": "kms:Decrypt*",
    "Resource": "*"
}
```

Como adicionar e ativar uma lista de entidades ou lista de IPs

Listas de entidades e listas de endereços IP ajudam você a personalizar os recursos de detecção de ameaças no GuardDuty. Para obter mais informações sobre essas listas, consulte Noções básicas sobre listas de entidades e listas de endereços IP. Para gerenciar os dados confiáveis e de inteligência contra ameaças do seu AWS ambiente, GuardDuty recomenda o uso de listas de entidades. Antes de começar, consulte Configuração de pré-requisitos para listas de entidades e listas de endereços IP.

Escolha um dos métodos de acesso a seguir para adicionar e habilitar uma lista de entidades confiável, uma lista de entidades de ameaças, uma lista de IPs confiáveis ou uma lista de IPs de ameaças.

Console

(Opcional) Etapa 1: buscar o URL do local da sua lista

1. Abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação, escolha Buckets.
3. Escolha o nome do bucket do Amazon S3 com a lista específica que deseja adicionar.
4. Escolha o nome do objeto (lista) para visualizar os respectivos detalhes.
5. Na guia Propriedades, copie o URI do S3 para esse objeto.

Etapa 2: adicionar dados confiáveis ou de inteligência contra ameaças

1. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.
2. No painel de navegação, escolha Listas de domínios.
3. Na página Listas, escolha a guia Listas de entidades ou Listas de endereços IP.
4. Com base na guia selecionada, escolha para adicionar uma lista confiável ou uma lista de ameaças.
5. Na caixa de diálogo para adicionar uma lista confiável ou de ameaças, faça o seguinte:

   a. Em Nome da lista, insira um nome para sua lista.

      Restrições de nomenclatura da lista — O nome da sua lista pode incluir letras minúsculas, letras maiúsculas, números, traço (-) e sublinhado (_).

      Para uma lista de endereços IP, o nome da sua lista deve ser exclusivo em uma região Conta da AWS e.

   b. Em Localização, informe o local em que o upload da sua lista foi realizado. Se você ainda não tiver configurado, consulte Step 1: Fetching location URL of your list.

      Aplica-se somente a ameaças personalizadas e conjuntos personalizados de entidades confiáveis – se você fornecer um URL de localização que não corresponda aos seguintes formatos compatíveis, receberá uma mensagem de erro durante a adição e ativação da lista.

      Formato do URL de localização:

      - https://s3.amazonaws.com/bucket.name/file.txt
      - https://s3-aws-region.amazonaws.com/bucket.name/file.txt
      - http://bucket.s3.amazonaws.com/file.txt
      - http://bucket.s3-aws-region.amazonaws.com/file.txt
      - s3://bucket. name/file.txt

   c. (Opcional) Para o proprietário esperado do bucket, você pode inserir o Conta da AWS ID que possui o bucket do Amazon S3 especificado no campo Localização.

      Quando você não especifica um proprietário de Conta da AWS ID, ele se GuardDuty comporta de maneira diferente para listas de entidades e listas de endereços IP. Para listas de entidades, GuardDuty validará se a conta membro atual é proprietária do bucket

do S3 especificado no campo Localização. Para listas de endereços IP, se você não especificar um proprietário de Conta da AWS ID, GuardDuty não realiza nenhuma validação.

Se GuardDuty descobrir que esse bucket do S3 não pertence ao ID de conta especificado, você receberá um erro no momento da ativação da lista.

d. Marque a caixa de seleção Concordo.

e. Escolha Adicionar lista. Por padrão, o Status da lista adicionada é Inativo. Para que a lista seja efetiva, você deve habilitá-la.

Etapa 3: ativar uma lista de entidades ou lista de endereços IP

1. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.
2. No painel de navegação, escolha Listas de domínios.
3. Na página Listas, selecione a guia na qual você deseja ativar a lista – Listas de entidades ou Listas de endereços IP.
4. Selecione uma lista que você deseja ativar. Isso habilitará o menu Ação e Editar.
5. Escolha Ações e Ativar.

API/CLI

Para adicionar e ativar uma lista de entidades confiáveis

1. Executar CreateTrustedEntitySet. Forneça o `detectorId` da conta de membro para a qual deseja criar essa lista de entidades confiáveis. Para encontrar o da `detectorId` sua conta e da região atual, consulte a página Configurações no https://console.aws.amazon.com/guardduty/ console ou execute a ListDetectors API.

   Restrições de nomenclatura da lista — O nome da sua lista pode incluir letras minúsculas, letras maiúsculas, números, traço (-) e sublinhado (_).

2. Outra alternativa é executar o seguinte comando da AWS Command Line Interface :

```
aws guardduty create-trusted-entity-set \
--detector-id 12abc34d567e8fa901bc2d34e56789f0 \
--name "AnyOrganizationListEXAMPLE" \
--format TXT \
```

```
--location "https://s3.amazonaws.com/amzn-s3-demo-bucket/DOC-EXAMPLE-SOURCE-
FILE.format" \
--activate
```

`detector-id`Substitua pelo ID do detector da conta membro para a qual você criará a lista de entidades confiáveis e outros valores de espaço reservado que sejam. *shown in red*

Se você não quiser ativar essa lista recém-criada, substitua o parâmetro `--activate` por `--no-activate`.

O parâmetro `expected-bucket-owner` é opcional. Se você especificar ou não o valor desse parâmetro, GuardDuty valida se o Conta da AWS ID associado a esse `--detector-id` valor possui o bucket do S3 especificado no `--location` parâmetro. Se GuardDuty descobrir que esse bucket do S3 não pertence ao ID de conta especificado, você receberá um erro no momento da ativação dessa lista.

Aplica-se somente a ameaças personalizadas e conjuntos personalizados de entidades confiáveis – se você fornecer um URL de localização que não corresponda aos seguintes formatos compatíveis, receberá uma mensagem de erro durante a adição e ativação da lista.

Para adicionar e ativar listas de entidades de ameaças

1. Executar CreateThreatEntitySet. Forneça o `detectorId` da conta de membro para a qual você deseja criar essa lista de entidades de ameaças. Para encontrar o da `detectorId` sua conta e da região atual, consulte a página Configurações no https://console.aws.amazon.com/guardduty/ console ou execute a ListDetectors API.

   Restrições de nomenclatura da lista — O nome da sua lista pode incluir letras minúsculas, letras maiúsculas, números, traço (-) e sublinhado (_).

2. Outra alternativa é executar o seguinte comando da AWS Command Line Interface :

```
aws guardduty create-threat-entity-set \
--detector-id 12abc34d567e8fa901bc2d34e56789f0 \
--name "AnyOrganizationListEXAMPLE" \
--format TXT \
--location "https://s3.amazonaws.com/amzn-s3-demo-bucket/DOC-EXAMPLE-SOURCE-
FILE.format" \
--activate
```

`detector-id`Substitua pelo ID do detector da conta membro para a qual você criará a lista de entidades confiáveis e outros valores de espaço reservado que sejam. *`shown in red`*

Se você não quiser ativar essa lista recém-criada, substitua o parâmetro `--activate` por `--no-activate`.

O parâmetro `expected-bucket-owner` é opcional. Se você especificar ou não o valor desse parâmetro, GuardDuty valida se o Conta da AWS ID associado a esse `--detector-id` valor possui o bucket do S3 especificado no `--location` parâmetro. Se GuardDuty descobrir que esse bucket do S3 não pertence ao ID de conta especificado, você receberá um erro no momento da ativação dessa lista.

Aplica-se somente a ameaças personalizadas e conjuntos personalizados de entidades confiáveis – se você fornecer um URL de localização que não corresponda aos seguintes formatos compatíveis, receberá uma mensagem de erro durante a adição e ativação da lista.

Para adicionar e ativar uma lista de endereços IPs confiáveis

1. Execute CreateIPSet. Forneça o `detectorId` da conta de membro para a qual deseja criar essa lista de endereços IPs confiáveis. Para encontrar o da `detectorId` sua conta e da região atual, consulte a página Configurações no https://console.aws.amazon.com/guardduty/ console ou execute a ListDetectors API.

   Para uma lista de endereços IP, o nome da sua lista deve ser exclusivo em uma região Conta da AWS e.

   Restrições de nomenclatura da lista — O nome da sua lista pode incluir letras minúsculas, letras maiúsculas, números, traço (-) e sublinhado (_).

2. Como alternativa, pode-se fazer isso executando o seguinte comando AWS Command Line Interface e substituindo `detector-id` pelo ID do detector da conta de membro para a qual a lista de endereços IPs confiáveis será atualizada.

```
aws guardduty create-ip-set \
--detector-id 12abc34d567e8fa901bc2d34e56789f0 \
--name "AnyOrganizationListEXAMPLE" \
--format TXT \
--location "https://s3.amazonaws.com/amzn-s3-demo-bucket/DOC-EXAMPLE-SOURCE-FILE.format" \
```

```
--activate
```

`detector-id`Substitua pela ID do detector da conta membro para a qual você criará a lista de IPs confiáveis e outros valores de espaço reservado que sejam. *shown in red*

Se você não quiser ativar essa lista recém-criada, substitua o parâmetro `--activate` por `--no-activate`.

O parâmetro `expected-bucket-owner` é opcional. Quando você não especifica o ID da conta que possui o bucket do S3, GuardDuty não realiza nenhuma validação. Quando você especifica a ID da conta para o `expected-bucket-owner` parâmetro, GuardDuty valida que essa Conta da AWS ID é proprietária do bucket do S3 especificado no `--location` parâmetro. Se GuardDuty descobrir que esse bucket do S3 não pertence ao ID de conta especificado, você receberá um erro no momento da ativação dessa lista.

Para adicionar e ativar listas de IP de ameaças

1. Executar CreateThreatIntelSet. Forneça o `detectorId` da conta de membro para a qual deseja criar essa lista de endereços IPs de ameaças. Para encontrar o da `detectorId` sua conta e da região atual, consulte a página Configurações no https://console.aws.amazon.com/guardduty/ console ou execute a ListDetectors API.

   Restrições de nomenclatura da lista — O nome da sua lista pode incluir letras minúsculas, letras maiúsculas, números, traço (-) e sublinhado (_).

   Para uma lista de endereços IP, o nome da sua lista deve ser exclusivo em uma região Conta da AWS e.

2. Como alternativa, pode-se fazer isso executando o seguinte comando AWS Command Line Interface e substituindo `detector-id` pelo ID do detector da conta de membro para a qual a lista de IPs confiáveis será atualizada.

```
aws guardduty create-threat-intel-set \
--detector-id 12abc34d567e8fa901bc2d34e56789f0 \
--name "AnyOrganizationListEXAMPLE" \
--format TXT \
--location "https://s3.amazonaws.com/amzn-s3-demo-bucket/DOC-EXAMPLE-SOURCE-FILE.format" \
--activate
```

`detector-id`Substitua pelo ID do detector da conta membro para a qual você criará a lista de IPs de ameaças e outros valores reservados que sejam. *`shown in red`*

Se você não quiser ativar essa lista recém-criada, substitua o parâmetro `--activate` por `--no-activate`.

O parâmetro `expected-bucket-owner` é opcional. Quando você não especifica o ID da conta que possui o bucket do S3, GuardDuty não realiza nenhuma validação. Quando você especifica a ID da conta para o `expected-bucket-owner` parâmetro, GuardDuty valida que essa Conta da AWS ID é proprietária do bucket do S3 especificado no `--location` parâmetro. Se GuardDuty descobrir que esse bucket do S3 não pertence ao ID de conta especificado, você receberá um erro no momento da ativação dessa lista.

Depois que você ativar uma lista de entidades ou de endereços IP, poderá levar alguns minutos para que essa lista entre em vigor. Para obter mais informações, consulte Considerações importantes sobre listas GuardDuty.

Atualizando uma lista de entidades ou lista de endereços IP

Listas de entidades e listas de endereços IP ajudam você a personalizar os recursos de detecção de ameaças no GuardDuty. Para obter mais informações sobre essas listas, consulte Noções básicas sobre listas de entidades e listas de endereços IP.

Você pode atualizar o nome de uma lista, a localização do bucket do S3, o ID esperado da conta do proprietário do bucket e as entradas em uma lista existente. Se você atualizar as entradas em uma lista, deverá seguir as etapas para ativar a lista novamente GuardDuty para usar a versão mais recente da lista. Depois que você atualizar ou ativar uma lista de entidades ou de endereços IP, poderá levar alguns minutos para que essa lista entre em vigor. Para obter mais informações, consulte Considerações importantes sobre listas GuardDuty.

> **Note**
>
> Se o status da lista for Ativando, Desativando ou Exclusão pendente, você deverá aguardar alguns minutos antes de realizar qualquer ação. Para informações sobre esses status, consulte Noções básicas sobre os status de listas.

Selecione um dos métodos de acesso para atualizar uma lista de entidades ou uma lista de endereços IP.

Console

1. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.
2. No painel de navegação, escolha Listas de domínios.
3. Na página Listas, escolha a guia apropriada Listas de entidades ou Listas de endereços IP.
4. Selecione uma lista (confiável ou de ameaças) que você deseja atualizar. Isso habilitará o menu Ação e Editar.
5. Escolha Editar.
6. Na caixa de diálogo para atualizar a lista, especifique os detalhes que você deseja atualizar.

   Restrições de nomenclatura da lista — O nome da sua lista pode incluir letras minúsculas, letras maiúsculas, números, traço (-) e sublinhado (_).

   Para uma lista de endereços IP, o nome da sua lista deve ser exclusivo em uma região Conta da AWS e.

   Aplica-se somente a ameaças personalizadas e conjuntos personalizados de entidades confiáveis – se você fornecer um URL de localização que não corresponda aos seguintes formatos compatíveis, receberá uma mensagem de erro durante a adição e ativação da lista.
7. (Opcional) Para Proprietário esperado do bucket, você pode inserir o Conta da AWS ID que possui o bucket do Amazon S3 especificado no campo Localização.

   Quando você não especifica um proprietário de Conta da AWS ID, ele se GuardDuty comporta de forma diferente para listas de entidades e listas de endereços IP. Para listas de entidades, GuardDuty validará se a conta do membro atual é proprietária do bucket S3 especificado no campo Localização. Para listas de endereços IP, se você não especificar um proprietário de Conta da AWS ID, GuardDuty não realiza nenhuma validação.

   Se GuardDuty descobrir que esse bucket do S3 não pertence ao ID da conta especificado, você receberá um erro no momento da ativação da lista.
8. Marque a caixa de seleção Concordo e, em seguida, selecione Atualizar lista.

API/CLI

Para começar com os procedimentos a seguir, você precisa do ID, como `trustedEntitySetId`, `threatEntitySetId`, `trustedIpSet` ou `threatIpSet`, que está associado ao recurso da lista que você deseja atualizar.

Para atualizar e ativar uma lista de entidades confiáveis

1. Executar UpdateTrustedEntitySet. Forneça o `detectorId` da conta de membro para a qual deseja atualizar essa lista de entidades confiáveis. Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no https://console.aws.amazon.com/guardduty/console ou execute a ListDetectorsAPI.

   Restrições de nomenclatura da lista — O nome da sua lista pode incluir letras minúsculas, letras maiúsculas, números, traço (-) e sublinhado (_).

2. Como alternativa, você pode fazer isso executando o seguinte comando AWS Command Line Interface que atualiza o `name` da lista e também ativa essa lista:

   ```
   aws guardduty update-trusted-entity-set \
   --detector-id 12abc34d567e8fa901bc2d34e56789f0 \
   --name "AnyOrganization ListEXAMPLE" \
   --trusted-entity-set-id d4b94fc952d6912b8f3060768example \
   --activate
   ```

   `detector-id`Substitua pelo ID do detector da conta do membro para a qual você criará a lista de entidades confiáveis e outros valores de espaço reservado que sejam*shown in red*.

   Se você não quiser ativar essa lista recém-criada, substitua o parâmetro `--activate` por `--no-activate`.

   O parâmetro `expected-bucket-owner` é opcional. Se você especificar ou não o valor desse parâmetro, GuardDuty valida se a Conta da AWS ID associada a esse `--detector-id` valor possui o bucket do S3 especificado no `--location` parâmetro. Se GuardDuty descobrir que esse bucket do S3 não pertence à ID da conta especificada, você receberá um erro no momento da ativação dessa lista.

Aplica-se somente a ameaças personalizadas e conjuntos personalizados de entidades confiáveis – se você fornecer um URL de localização que não corresponda aos seguintes formatos compatíveis, receberá uma mensagem de erro durante a adição e ativação da lista.

Para atualizar e ativar uma lista de entidades de ameaças

1. Executar UpdateThreatEntitySet. Forneça o `detectorId` da conta de membro para a qual você deseja criar essa lista de entidades de ameaças. Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no https://console.aws.amazon.com/guardduty/console ou execute a ListDetectorsAPI.

   Restrições de nomenclatura da lista — O nome da sua lista pode incluir letras minúsculas, letras maiúsculas, números, traço (-) e sublinhado (_).
2. Como alternativa, você pode fazer isso executando o seguinte comando AWS Command Line Interface que atualiza o `name` da lista e também ativa essa lista:

   ```
   aws guardduty update-threat-entity-set \
   --detector-id 12abc34d567e8fa901bc2d34e56789f0 \
   --name "AnyOrganization ListEXAMPLE" \
   --threat-entity-set-id d4b94fc952d6912b8f3060768example \
   --activate
   ```

   `detector-id`Substitua pelo ID do detector da conta do membro para a qual você criará a lista de entidades ameaçadoras e outros valores de espaço reservado que estejam*shown in red*.

   Se você não quiser ativar essa lista recém-criada, substitua o parâmetro `--activate` por `--no-activate`.

   O parâmetro `expected-bucket-owner` é opcional. Se você especificar ou não o valor desse parâmetro, GuardDuty valida se a Conta da AWS ID associada a esse `--detector-id` valor possui o bucket do S3 especificado no `--location` parâmetro. Se GuardDuty descobrir que esse bucket do S3 não pertence à ID da conta especificada, você receberá um erro no momento da ativação dessa lista.

   Aplica-se somente a ameaças personalizadas e conjuntos personalizados de entidades confiáveis – se você fornecer um URL de localização que não corresponda aos seguintes formatos compatíveis, receberá uma mensagem de erro durante a adição e ativação da lista.

Para atualizar e ativar uma lista de endereços IPs confiáveis

1. Execute CreateIPSet. Forneça o `detectorId` da conta de membro para a qual deseja atualizar essa lista de endereços IP confiáveis. Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no https://console.aws.amazon.com/guardduty/console ou execute a ListDetectorsAPI.

   Restrições de nomenclatura da lista — O nome da sua lista pode incluir letras minúsculas, letras maiúsculas, números, traço (-) e sublinhado (_).

   Para uma lista de endereços IP, o nome da sua lista deve ser exclusivo em uma região Conta da AWS e.

2. Como alternativa, você pode fazer isso executando o seguinte comando AWS Command Line Interface que também ativa a lista:

   ```
   aws guardduty update-ip-set \
   --detector-id 12abc34d567e8fa901bc2d34e56789f0 \
   --name "AnyOrganization ListEXAMPLE" \
   --ip-set-id d4b94fc952d6912b8f3060768example \
   --activate
   ```

   `detector-id`Substitua pelo ID do detector da conta do membro para a qual você atualizará a lista de IPs confiáveis e outros valores de espaço reservado que estejam*shown in red*.

   Se você não quiser ativar essa lista recém-criada, substitua o parâmetro `--activate` por `--no-activate`.

   O parâmetro `expected-bucket-owner` é opcional. Quando você não especifica o ID da conta que possui o bucket do S3, GuardDuty não realiza nenhuma validação. Quando você especifica a ID da conta para o `expected-bucket-owner` parâmetro, GuardDuty valida se essa Conta da AWS ID é proprietária do bucket do S3 especificado no `--location` parâmetro. Se GuardDuty descobrir que esse bucket do S3 não pertence à ID da conta especificada, você receberá um erro no momento da ativação dessa lista.

Para adicionar e ativar listas de IP de ameaças

1. Executar CreateThreatIntelSet. Forneça o `detectorId` da conta de membro para a qual deseja criar essa lista de endereços IPs de ameaças. Para encontrar a opção

`detectorId` para sua conta e região atual, consulte a página de configurações no https://console.aws.amazon.com/guardduty/console ou execute a ListDetectorsAPI.

Restrições de nomenclatura da lista — O nome da sua lista pode incluir letras minúsculas, letras maiúsculas, números, traço (-) e sublinhado (_).

Para uma lista de endereços IP, o nome da sua lista deve ser exclusivo em uma região Conta da AWS e.

2. Como alternativa, você pode fazer isso executando o seguinte comando AWS Command Line Interface que também ativa a lista:

```
aws guardduty update-threat-intel-set \
--detector-id 12abc34d567e8fa901bc2d34e56789f0 \
--name "AnyOrganization ListEXAMPLE" \
--threat-intel-set-id d4b94fc952d6912b8f3060768example \
--activate
```

`detector-id`Substitua pelo ID do detector da conta do membro para a qual você atualizará a lista de IPs de ameaças e outros valores de espaço reservado que estejam*shown in red*.

Se você não quiser ativar essa lista recém-criada, substitua o parâmetro `--activate` por `--no-activate`.

O parâmetro `expected-bucket-owner` é opcional. Quando você não especifica o ID da conta que possui o bucket do S3, GuardDuty não realiza nenhuma validação. Quando você especifica a ID da conta para o `expected-bucket-owner` parâmetro, GuardDuty valida se essa Conta da AWS ID é proprietária do bucket do S3 especificado no `--location` parâmetro. Se GuardDuty descobrir que esse bucket do S3 não pertence à ID da conta especificada, você receberá um erro no momento da ativação dessa lista.

De-activating lista de entidades ou lista de endereços IP

Quando você não quiser mais GuardDuty usar uma lista, poderá desativá-la. O processo pode levar alguns minutos para ser concluído. Para obter mais informações, consulte Considerações importantes sobre listas GuardDuty. Depois que a lista for desativada, as entradas na lista de entidades ou na lista de endereços IP não afetarão a detecção de ameaças em GuardDuty.

Selecione um dos métodos de acesso para desativar a lista.

Console

Para desativar uma lista de entidades ou lista de endereços IP

1. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.
2. No painel de navegação, escolha Listas de domínios.
3. Na página Lista, selecione a guia na qual você deseja desativar a lista – Listas de entidades ou Listas de endereços IP.
4. Na guia selecionada, selecione a lista que você deseja desativar.
5. Escolha Ações e Desativar.
6. Confirme a ação e escolha Desativar.

API/CLI

Para começar com os procedimentos a seguir, você precisa do ID, como `trustedEntitySetId`, `threatEntitySetId`, `trustedIpSet` ou `threatIpSet`, que está associado ao recurso da lista que você deseja desativar.

Para desativar uma lista de entidades confiáveis

1. Executar UpdateTrustedEntitySet. Forneça o `detectorId` da conta de membro para a qual deseja desativar essa lista de entidades confiáveis. Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no https://console.aws.amazon.com/guardduty/console ou execute a ListDetectorsAPI.
2. Outra alternativa é executar o seguinte comando da AWS Command Line Interface :

```
aws guardduty update-trusted-entity-set \
--detector-id 12abc34d567e8fa901bc2d34e56789f0 \
--trusted-entity-set-id d4b94fc952d6912b8f3060768example \
--no-activate
```

`detector-id`Substitua pelo ID do detector da conta do membro para a qual você desativará a lista de entidades confiáveis e outros valores de espaço reservado que estejam. *`shown in red`*

Para desativar listas de entidades de ameaças

1. Executar UpdateThreatEntitySet. Forneça o `detectorId` da conta de membro para a qual deseja desativar essa lista de entidades de ameaças. Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no https://console.aws.amazon.com/guardduty/console ou execute a ListDetectorsAPI.
2. Outra alternativa é executar o seguinte comando da AWS Command Line Interface :

```
aws guardduty update-threat-entity-set \
--detector-id 12abc34d567e8fa901bc2d34e56789f0 \
--threat-entity-set-id d4b94fc952d6912b8f3060768example \
--no-activate
```

`detector-id`Substitua pelo ID do detector da conta do membro para a qual você criará a lista de entidades ameaçadoras e outros valores de espaço reservado que estejam*shown in red*.

Para desativar uma lista de endereços IP confiáveis

1. Execute UpdateIPSet. Forneça o `detectorId` da conta de membro para a qual deseja desativar essa lista de endereços IP confiáveis. Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no https://console.aws.amazon.com/guardduty/console ou execute a ListDetectorsAPI.
2. Como alternativa, pode-se fazer isso executando o seguinte comando AWS Command Line Interface e substituindo `detector-id` pelo ID do detector da conta de membro para a qual a lista de endereços IPs confiáveis será desativada.

```
aws guardduty update-ip-set \
--detector-id 12abc34d567e8fa901bc2d34e56789f0 \
--ip-set-id d4b94fc952d6912b8f3060768example \
--no-activate
```

Para desativar a lista de IPs de ameaças

1. Executar UpdateThreatIntelSet. Forneça o `detectorId` da conta de membro para a qual deseja desativar essa lista de endereços IP de ameaças. Para encontrar a opção

`detectorId` para sua conta e região atual, consulte a página de configurações no https://console.aws.amazon.com/guardduty/console ou execute a ListDetectorsAPI.

2. Como alternativa, pode-se fazer isso executando o seguinte comando AWS Command Line Interface e substituindo `detector-id` pelo ID do detector da conta de membro para a qual a lista de IPs de ameaças será desativada.

```
aws guardduty update-threat-intel-set \
--detector-id 12abc34d567e8fa901bc2d34e56789f0 \
--threat-intel-set-id d4b94fc952d6912b8f3060768example \
--no-activate
```

Excluindo lista de entidades ou lista de endereços IP

Quando você não quiser mais manter uma entrada de listas em seu conjunto de entidades ou de endereços IP, exclua-a. O processo pode levar alguns minutos para ser concluído. Para obter mais informações, consulte Considerações importantes sobre listas GuardDuty.

Se o status da lista for Ativando ou Desativando, você deverá aguardar alguns minutos antes de realizar qualquer ação. Para obter mais informações, consulte Noções básicas sobre os status de listas.

Selecione um dos métodos de acesso para excluir a lista.

Console

Para excluir a lista de entidades ou de endereços IP

1. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.
2. No painel de navegação, escolha Listas de domínios.
3. Na página Lista, selecione a guia na qual você deseja excluir a lista – Listas de entidades ou Listas de endereços IP.
4. Na guia selecionada, selecione a lista que você deseja excluir.
5. Escolha Ações e, em seguida, escolha Excluir.

   O status da lista mudará para Excluir pendente. Pode levar alguns minutos para que a lista seja excluída.

API/CLI

Para começar com os procedimentos a seguir, você precisa do ID, como `trustedEntitySetId`, `threatEntitySetId`, `trustedIpSet` ou `threatIpSet`, que está associado ao recurso da lista que você deseja excluir.

Para excluir uma lista de entidades confiáveis

1. Executar DeleteTrustedEntitySet. Forneça o `detectorId` da conta de membro para a qual deseja excluir essa lista de entidades confiáveis. Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no https://console.aws.amazon.com/guardduty/console ou execute a ListDetectorsAPI.
2. Outra alternativa é executar o seguinte comando da AWS Command Line Interface :

```
aws guardduty delete-trusted-entity-set \
--detector-id 12abc34d567e8fa901bc2d34e56789f0 \
--trusted-entity-set-id d4b94fc952d6912b8f3060768example
```

`detector-id`Substitua pelo ID do detector da conta do membro da qual você excluirá a lista de entidades confiáveis e outros valores de espaço reservado que estejam*shown in red*.

Para desativar listas de entidades de ameaças

1. Executar DeleteThreatEntitySet. Forneça o `detectorId` da conta de membro para a qual deseja excluir essa lista de entidades de ameaças. Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no https://console.aws.amazon.com/guardduty/console ou execute a ListDetectorsAPI.
2. Outra alternativa é executar o seguinte comando da AWS Command Line Interface :

```
aws guardduty delete-threat-entity-set \
--detector-id 12abc34d567e8fa901bc2d34e56789f0 \
--threat-entity-set-id d4b94fc952d6912b8f3060768example
```

`detector-id`Substitua pelo ID do detector da conta do membro da qual você excluirá a lista de entidades ameaçadoras e outros valores de espaço reservado que estejam*shown in red*.

Para excluir uma lista de endereços IP confiáveis

1. Execute DeleteIPset. Forneça o `detectorId` da conta de membro para a qual deseja excluir essa lista de endereços IP confiáveis. Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no https://console.aws.amazon.com/guardduty/console ou execute a ListDetectorsAPI.
2. Como alternativa, pode-se fazer isso executando o comando AWS Command Line Interface a seguir e substituindo `detector-id` pelo ID do detector da conta de membro para a qual a lista de endereços IPs confiáveis será excluída.

```
aws guardduty delete-ip-set \
--detector-id 12abc34d567e8fa901bc2d34e56789f0 \
--ip-set-id d4b94fc952d6912b8f3060768example
```

`detector-id`Substitua pelo ID do detector da conta do membro da qual você excluirá a lista de entidades ameaçadoras e outros valores de espaço reservado que estejam*shown in red*.

Para excluir a lista de IPs de ameaças

1. Executar DeleteThreatIntelSet. Forneça o `detectorId` da conta de membro para a qual deseja excluir essa lista de endereços IP de ameaças. Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no https://console.aws.amazon.com/guardduty/console ou execute a ListDetectorsAPI.
2. Como alternativa, pode-se fazer isso executando o seguinte comando AWS Command Line Interface e substituindo `detector-id` pelo ID do detector da conta de membro para a qual a lista de IPs de ameaças será excluída.

```
aws guardduty delete-threat-intel-set \
--detector-id 12abc34d567e8fa901bc2d34e56789f0 \
--threat-intel-set-id d4b94fc952d6912b8f3060768example
```

`detector-id`Substitua pelo ID do detector da conta do membro da qual você excluirá a lista de entidades ameaçadoras e outros valores de espaço reservado que estejam*shown in red*.

Exportação de GuardDuty descobertas geradas para buckets do Amazon S3

GuardDuty retém as descobertas geradas por um período de 90 dias. GuardDuty exporta as descobertas ativas para a Amazon EventBridge (EventBridge). Opcionalmente, pode-se exportar as descobertas geradas para um bucket do Amazon Simple Storage Service (Amazon S3). Isso ajudará você a rastrear dados históricos de possíveis atividades suspeitas em sua conta e avaliar se as etapas de remediação recomendadas foram bem-sucedidas.

Todas as novas descobertas ativas GuardDuty geradas são exportadas automaticamente em cerca de 5 minutos após a geração da descoberta. Você pode definir a frequência com que as atualizações das descobertas ativas são exportadas EventBridge. A frequência que você seleciona se aplica à exportação de novas ocorrências de descobertas existentes para EventBridge seu bucket S3 (quando configurado) e Detective (quando integrado). Para obter informações sobre como GuardDuty agrega várias ocorrências de descobertas existentes, consulte. GuardDuty encontrando agregação

Quando você define as configurações para exportar descobertas para um bucket do Amazon S3, GuardDuty usa AWS Key Management Service (AWS KMS) para criptografar os dados das descobertas em seu bucket do S3. Isso exige que você adicione permissões ao seu bucket do S3 e à AWS KMS chave para que ele GuardDuty possa usá-las para exportar descobertas em sua conta.

Conteúdo

- Considerações
- Etapa 1: Permissões necessárias para configurar a exportação de descobertas
- Etapa 2: Anexar política à sua chave do KMS
- Etapa 3: Anexar uma política ao bucket Amazon S3
- Etapa 4: Exportar descobertas para um bucket do S3 (console)
- Etapa 5: Definir a frequência para exportar descobertas ativas atualizadas

Considerações

Antes de prosseguir com os pré-requisitos e as etapas para exportar as descobertas, considere os seguintes conceitos-chave:

- As configurações de exportação são regionais — você precisa configurar as opções de exportação em cada região em que você usa GuardDuty.
- Exportar descobertas para buckets do Amazon S3 em diferentes Regiões da AWS (entre regiões) — GuardDuty suporta as seguintes configurações de exportação:
  - Seu bucket ou objeto do Amazon S3 e sua AWS KMS chave devem pertencer ao mesmo Região da AWS.
  - Para as descobertas geradas em uma região comercial, é possível optar por exportar essas descobertas para um bucket S3 em qualquer região comercial. No entanto, você não pode exportar essas descobertas para um bucket S3 em uma região de adesão.
  - Para as descobertas geradas em uma região de aceitação, é possível optar por exportar essas descobertas para a mesma região de aceitação em que foram geradas ou para qualquer região comercial. No entanto, não é possível exportar as descobertas de uma região de opt-in para outra região de opt-in.
- Permissões para exportar descobertas — Para definir as configurações para exportar descobertas ativas, seu bucket do S3 deve ter permissões que permitam GuardDuty fazer upload de objetos. Você também deve ter uma AWS KMS chave que GuardDuty possa ser usada para criptografar descobertas.
- Descobertas arquivadas não exportadas: o comportamento padrão é que as descobertas arquivadas, incluindo novas instâncias de descobertas suprimidas, não sejam exportadas.

  Quando uma GuardDuty descoberta for gerada como arquivada, você precisará desarquivá-la. Isso altera o status de busca do filtro para Ativo. GuardDuty exporta as atualizações para as descobertas não arquivadas existentes com base em como você configura. Etapa 5 — Frequência de exportação de descobertas
- GuardDuty conta de administrador pode exportar descobertas geradas em contas de membros associadas — Quando você configura a exportação de descobertas em uma conta de administrador, todas as descobertas das contas de membros associadas geradas na mesma região também são exportadas para o mesmo local que você configurou para a conta de administrador. Para obter mais informações, consulte Entendendo a relação entre a conta GuardDuty do administrador e as contas dos membros.

Etapa 1: Permissões necessárias para configurar a exportação de descobertas

Ao definir as configurações para exportar descobertas, você seleciona um bucket do Amazon S3 onde você pode armazenar as descobertas e uma AWS KMS chave para usar na criptografia de dados. Além das permissões para GuardDuty ações, você também deve ter permissões para as seguintes ações para definir com êxito as configurações para exportar descobertas:

- `s3:GetBucketLocation`
- `s3:PutObject`

Se você precisar exportar as descobertas para um prefixo específico em seu bucket do Amazon S3, você também deve adicionar as seguintes permissões ao perfil do IAM:

- `s3:GetObject`
- `s3:ListBucket`

Etapa 2: Anexar política à sua chave do KMS

GuardDuty criptografa os dados das descobertas em seu bucket usando AWS Key Management Service. Para definir as configurações com êxito, primeiro você deve dar GuardDuty permissão para usar uma chave KMS. Você pode conceder as permissões anexando a política à sua chave do KMS.

Ao usar uma chave KMS de outra conta, você precisa aplicar a política de chaves fazendo login no Conta da AWS proprietário da chave. Ao configurar para exportar descobertas, você também precisará da chave ARN dessa conta que possui a chave.

Para modificar a política de chaves do KMS para GuardDuty criptografar suas descobertas exportadas

1. Abra o AWS KMS console em https://console.aws.amazon.com/kms.
2. Para alterar o Região da AWS, use o seletor de região no canto superior direito da página.
3. Selecione uma chave KMS existente ou execute as etapas para Criar uma nova chave no Guia do desenvolvedor do AWS Key Management Service , que você usará para criptografar as descobertas exportadas.

> **Note**
>
> A chave Região da AWS do KMS e o bucket do Amazon S3 devem ser iguais.

Use o mesmo bucket do S3 e o mesmo par de chaves KMS para exportar as descobertas de qualquer região aplicável. Para obter mais informações, consulte Considerações para exportar descobertas do entre regiões.

4. Na seção Política de chave escolha Editar.

   Se Mudar para visualização da política for exibido, selecione-o para exibir a Política de chave e, em seguida, escolha Editar.

5. Copie o seguinte bloco de política para sua política de chaves KMS para conceder GuardDuty permissão para usar sua chave.

```
{
    "Sid": "AllowGuardDutyKey",
    "Effect": "Allow",
    "Principal": {
        "Service": "guardduty.amazonaws.com"
    },
    "Action": "kms:GenerateDataKey",
    "Resource": "KMS key ARN",
    "Condition": {
        "StringEquals": {
            "aws:SourceAccount": "123456789012",
            "aws:SourceArn":
 "arn:aws:guardduty:Region2:123456789012:detector/SourceDetectorID"
        }
    }
}
```

6. Edite a política substituindo os seguintes valores que estão formatados *red* no exemplo de política:

   1. *KMS key ARN*Substitua pelo nome de recurso da Amazon (ARN) da chave KMS. Para saber como localizar o ARN da chave, consulte Localizar o ID da chave e o ARN no Guia do desenvolvedor do AWS Key Management Service .

2. *123456789012*Substitua pelo Conta da AWS ID que possui a GuardDuty conta que exporta as descobertas.
3. *Region2*Substitua pelo Região da AWS local onde as GuardDuty descobertas são geradas.
4. *SourceDetectorID*Substitua pelo `detectorID` da GuardDuty conta na região específica em que as descobertas foram geradas.

   Para encontrar o da `detectorId` sua conta e da região atual, consulte a página Configurações no https://console.aws.amazon.com/guardduty/ console ou execute a ListDetectors API.

> **Note**
>
> Se você estiver usando GuardDuty em uma região opcional, substitua o valor do "Serviço" pelo endpoint regional dessa região. Por exemplo, se você estiver usando GuardDuty na região do Oriente Médio (Bahrein) (me-south-1), substitua por. `"Service": "guardduty.amazonaws.com"` `"Service": "guardduty.me-south-1.amazonaws.com"` Para obter informações sobre endpoints para cada região de aceitação, consulte GuardDuty Endpoints e cotas.

7. Se você adicionou a declaração de política antes da declaração final, adicione uma vírgula antes de adicionar essa declaração. Certifique-se de que a sintaxe JSON da sua política de chaves do KMS seja válida.

   Escolha Salvar.
8. (Opcional) copie o ARN da chave em um bloco de notas para uso nas etapas posteriores.

Etapa 3: Anexar uma política ao bucket Amazon S3

Adicione permissões ao bucket do Amazon S3 para o qual você exportará as descobertas para que GuardDuty possa fazer upload de objetos para esse bucket do S3. Independentemente de usar um bucket do Amazon S3 que pertença à sua conta ou a outra Conta da AWS, você deve adicionar essas permissões.

Caso, em algum momento, as descobertas sejam exportadas para um bucket S3 diferente, para continuar exportando as descobertas, será necessário adicionar permissões a esse bucket do S3 e definir novamente as configurações de exportação de descobertas.

Se você ainda não tem um bucket do Amazon S3 para o qual deseja exportar essas descobertas, consulte Criação de um bucket no Guia do usuário do Amazon S3.

Anexar permissões a sua política de bucket do S3

1. Execute as etapas em Para criar ou editar uma política de bucket no Guia do usuário do Amazon S3, até que a página Editar política de bucket seja exibida.
2. O exemplo de política mostra como conceder GuardDuty permissão para exportar descobertas para seu bucket do Amazon S3. Caso altere o caminho depois de configurar a exportação de descobertas, você deve modificar a política para conceder permissão para o novo local.

   Copie a política de exemplo a seguir e cole-a no Editor de políticas do bucket.

   Se você adicionou a declaração de política antes da declaração final, adicione uma vírgula antes de adicionar essa declaração. Certifique-se de que a sintaxe JSON da sua política de chaves do KMS seja válida.

   Exemplo de política de bucket do S3

   JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "Allow GetBucketLocation",
            "Effect": "Allow",
            "Principal": {
                "Service": "guardduty.amazonaws.com"
            },
            "Action": "s3:GetBucketLocation",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "123456789012",
                    "aws:SourceArn": "arn:aws:guardduty:us-
east-2:123456789012:detector/SourceDetectorID"

                }
            }
        },
```

```
        {
            "Sid": "Allow PutObject",
            "Effect": "Allow",
            "Principal": {
                "Service": "guardduty.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket[optional prefix]/
*",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "123456789012",
                    "aws:SourceArn": "arn:aws:guardduty:us-
east-2:123456789012:detector/SourceDetectorID"

                }
            }
        },
        {
            "Sid": "Deny unencrypted object uploads",
            "Effect": "Deny",
            "Principal": {
                "Service": "guardduty.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket[optional prefix]/
*",
            "Condition": {
                "StringNotEquals": {
                    "s3:x-amz-server-side-encryption": "aws:kms"
                }
            }
        },
        {
            "Sid": "Deny incorrect encryption header",
            "Effect": "Deny",
            "Principal": {
                "Service": "guardduty.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket[optional prefix]/
*",
            "Condition": {
                "StringNotEquals": {
```

```
                "s3:x-amz-server-side-encryption-aws-kms-key-id":
 "arn:aws:kms:us-east-2:111122223333:key/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111"
                }
            }
        },
        {
            "Sid": "Deny non-HTTPS access",
            "Effect": "Deny",
            "Principal": "*",
            "Action": "s3:*",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket[optional prefix]/
*",
            "Condition": {
                "Bool": {
                    "aws:SecureTransport": "false"
                }
            }
        }
    ]
}
```

3. Edite a política substituindo os seguintes valores que estão formatados *red* no exemplo de política:

   1. *Amazon S3 bucket ARN*Substitua pelo nome de recurso da Amazon (ARN) do bucket do Amazon S3. Você pode encontrar o ARN do bucket na página Editar política do bucket no https://console.aws.amazon.com/s3/ console.
   2. *123456789012*Substitua pelo Conta da AWS ID que possui a GuardDuty conta que exporta as descobertas.
   3. *us-east-2*Substitua pelo Região da AWS local onde as GuardDuty descobertas são geradas.
   4. *SourceDetectorID*Substitua pelo `detectorID` da GuardDuty conta na região específica em que as descobertas foram geradas.

      Para encontrar o da `detectorId` sua conta e da região atual, consulte a página Configurações no https://console.aws.amazon.com/guardduty/ console ou execute a ListDetectors API.
   5. Substitua *[optional prefix]* parte do valor do *S3 bucket ARN/[optional prefix]* espaço reservado por um local de pasta opcional para o qual você deseja exportar as

descobertas. Para obter mais informações sobre ouso de prefixos, consulte Organizando objetos usando prefixos no Guia de usuário do Amazon S3.

Quando você fornece um local de pasta opcional, a pasta já deve existir no bucket do S3. GuardDuty não cria a pasta em seu nome. Esse requisito se aplica independentemente da propriedade do bucket.

6. *KMS key ARN*Substitua pelo nome de recurso da Amazon (ARN) da chave KMS associada à criptografia das descobertas exportadas para o bucket do S3. Para saber como localizar o ARN da chave, consulte Localizar o ID da chave e o ARN no Guia do desenvolvedor do AWS Key Management Service .

> **Note**
>
> Se você estiver usando GuardDuty em uma região opcional, substitua o valor do "Serviço" pelo endpoint regional dessa região. Por exemplo, se você estiver usando GuardDuty na região do Oriente Médio (Bahrein) (me-south-1), substitua por. `"Service": "guardduty.amazonaws.com"` `"Service": "guardduty.me-south-1.amazonaws.com"` Para obter informações sobre endpoints para cada região de aceitação, consulte GuardDuty Endpoints e cotas.

4. Escolha Salvar.

Etapa 4: Exportar descobertas para um bucket do S3 (console)

GuardDuty permite que você exporte descobertas para um bucket existente em outro Conta da AWS.

Ao criar um novo bucket S3 ou escolher um bucket existente em sua conta, é possível adicionar um prefixo. Tanto o prefixo quanto o caminho da pasta em que as descobertas são gravadas já devem existir no bucket do S3. GuardDuty não cria nenhuma pasta em seu nome. GuardDuty grava objetos de descobertas no caminho`/AWSLogs/`*`123456789012`*`/GuardDuty/`*`Region`*, portanto, você deve criar essa estrutura de pastas antes de exportar as descobertas.

Todo o caminho do objeto S3 será *`amzn-s3-demo-bucket`*`/`*`prefix-name`*`/UUID`*`.jsonl.gz`*. O `UUID` é gerado aleatoriamente e não representa o ID do detector ou o ID da descoberta.

> **Important**
>
> A chave do KMS e o bucket do S3 devem estar na mesma região.

Antes de concluir essas etapas, verifique se as respectivas políticas foram anexadas à chave KMS e ao bucket do S3 existente.

Para configurar a opção exportar descobertas

1. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.
2. No painel de navegação, selecione Configurações.
3. Na página Configurações, em Opções de exportação de descobertas, para o bucket do S3, escolha Configurar agora (ou Editar, conforme necessário).
4. Para ARN de bucket S3, insira o **`bucket ARN`**. Para encontrar o ARN do bucket, consulte Visualização das propriedades de um bucket do S3 no Guia do usuário do Amazon S3.
5. Para o ARN da chave KMS, digite o **`key ARN`**. Para saber como localizar o ARN da chave, consulte Localizar o ID da chave e o ARN no Guia do desenvolvedor do AWS Key Management Service .
6. Anexar políticas
   - Execute as etapas para anexar a política de bucket do S3. Para obter mais informações, consulte Etapa 3: Anexar uma política ao bucket Amazon S3.
   - Execute as etapas para anexar a política de chave do KMS. Para obter mais informações, consulte Etapa 2: Anexar política à sua chave do KMS.
7. Escolha Salvar.

Etapa 5: Definir a frequência para exportar descobertas ativas atualizadas

Configure a frequência para exportar descobertas ativas atualizadas conforme apropriado para seu ambiente. Por padrão, as descobertas atualizadas são exportadas a cada 6 horas. Isso significa que todas as descobertas que forem atualizadas após a exportação mais recente serão incluídas na próxima exportação. Se as descobertas atualizadas forem exportadas a cada 6 horas e a exportação ocorrer às 12h, todas as descobertas atualizadas após 12h serão exportadas às 18h.

Como definir a frequência

1. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.
2. Escolha Configurações.
3. Na seção Opções de exportação de descobertas, selecione Frequência para descobertas atualizadas. Isso define a frequência de exportação de descobertas ativas atualizadas para o Amazon S3 EventBridge e para o Amazon S3. Você pode escolher entre as seguintes opções:
   - Atualização EventBridge e S3 a cada 15 minutos
   - Atualização EventBridge e S3 a cada 1 hora
   - Atualização EventBridge e S3 a cada 6 horas (padrão)
4. Escolha Salvar alterações.

Processando GuardDuty descobertas com a Amazon EventBridge

GuardDuty publica (envia) automaticamente descobertas como eventos para a Amazon EventBridge (antiga Amazon CloudWatch Events), um serviço de ônibus de eventos sem servidor. EventBridge fornece um fluxo de dados quase em tempo real de aplicativos e serviços para destinos como tópicos AWS Lambda , funções e streams do Amazon Kinesis Notification Service (Amazon SNS). Para obter mais informações, consulte o Guia EventBridge do usuário da Amazon.

EventBridge permite o monitoramento e o processamento GuardDuty automatizados das descobertas por meio do recebimento de eventos. EventBridge recebe eventos tanto para descobertas recém-geradas quanto para descobertas agregadas, em que ocorrências subsequentes de uma descoberta existente são combinadas com a original. Cada GuardDuty descoberta recebe uma ID de descoberta e GuardDuty cria um EventBridge evento para cada descoberta com uma ID de descoberta exclusiva. Para obter informações sobre como a agregação funciona em GuardDuty, consulteGuardDuty encontrando agregação.

Além do monitoramento e processamento automatizados, o uso de EventBridge permite a retenção de longo prazo dos dados de suas descobertas. GuardDuty armazena as descobertas por 90 dias. Com EventBridge, você pode enviar dados de descobertas para sua plataforma de armazenamento preferida e armazenar os dados pelo tempo que quiser. Para reter as descobertas por um longo período, GuardDuty suportaExportar as descobertas geradas para bucket do Amazon S3.

Tópicos

- Entendendo a frequência de EventBridge notificação em GuardDuty

- Configurar um tópico e um endpoint do Amazon SNS (e-mail, Slack e Amazon Chime)
- Usando a Amazon EventBridge para GuardDuty descobertas
- Criação de uma EventBridge regra para GuardDuty descobertas
- EventBridge regra para ambientes GuardDuty com várias contas

Entendendo a frequência de EventBridge notificação em GuardDuty

Esta seção explica com que frequência você recebe notificações de busca EventBridge e como atualizar a frequência para ocorrências de busca subsequentes.

Notificações de descobertas recém-geradas com um ID de descoberta exclusivo

GuardDuty envia essas notificações quase em tempo real quando gera uma descoberta com um ID de descoberta exclusivo. A notificação inclui todas as ocorrências subsequentes dessa ID de descoberta durante o processo de geração da notificação.

A frequência das notificações das descobertas recém-geradas é quase em tempo real. Por padrão, você não pode modificar essa frequência.

Notificações para ocorrências de descoberta subsequentes

GuardDuty agrega todas as ocorrências subsequentes de um determinado tipo de descoberta que ocorrem dentro dos intervalos de 6 horas em um único evento. Somente uma conta de administrador pode atualizar a frequência de EventBridge notificação para ocorrências de busca subsequentes. Uma conta de membro não pode atualizar essa frequência em sua própria conta. Por exemplo, se a conta do GuardDuty administrador delegado atualizar a frequência para uma hora, todas as contas dos membros também terão uma frequência de notificação de uma hora sobre as ocorrências de descoberta subsequentes enviadas para. EventBridge Para obter mais informações, consulte Gerenciando várias contas na Amazon GuardDuty.

Como uma conta de administrador, você pode personalizar a frequência padrão das notificações sobre as ocorrências de descobertas subsequentes. Valores possíveis são 15 minutos, 1 hora ou 6 horas (padrão). Para obter informações sobre como definir a frequência dessas notificações, consulte Etapa 5: Definir a frequência para exportar descobertas ativas atualizadas.

Para obter mais detalhes sobre a conta de administrador recebendo EventBridge notificações para contas de membros, consulteEventBridge regra para ambientes com várias contas.

Configurar um tópico e um endpoint do Amazon SNS (e-mail, Slack e Amazon Chime)

O Amazon Simple Notification Service (Amazon SNS) é um serviço totalmente gerenciado que fornece entrega de mensagens de publicadores para assinantes. Os publicadores se comunicam de maneira assíncrona com os assinantes enviando mensagens para um tópico. Um tópico é um ponto de acesso lógico e um canal de comunicação que permite agrupar vários endpoints AWS Lambda, como Amazon Simple Queue Service (Amazon HTTP/S SQS) e um endereço de e-mail.

> **Note**
>
> Você pode adicionar um tópico do Amazon SNS à sua regra de EventBridge evento preferida durante ou após a criação da regra.

Criar um tópico do Amazon SNS

Para começar, você deve primeiro configurar um tópico no Amazon SNS e adicionar um endpoint. Para criar um tópico, consulte as etapas em Etapa 1: criar um tópico no Guia do desenvolvedor do Amazon Simple Notification Service. Depois que o tópico for criado, copie o ARN do tópico para a área de transferência. Você usará esse ARN de tópico para continuar com uma das configurações preferidas.

Escolha um método preferido para estabelecer para onde você deseja enviar os dados de GuardDuty busca.

Email setup

Para configurar um endpoint de e-mail

Depois que você Create an Amazon SNS topic, a próxima etapa é criar uma assinatura para esse tópico. Siga as etapas em Etapa 2: criar uma assinatura para um tópico do Amazon SNS no Guia do desenvolvedor do Amazon Simple Notification Service.

1. Para ARN de tópico, use o ARN do tópico criado na etapa Create an Amazon SNS topic. O ARN do tópico é semelhante ao seguinte:

```
arn:aws:sns:us-east-2:123456789012:your_topic
```

2. Em Protocol (Protocolo), selecione Email.
3. Para Endpoint, insira um endereço de e-mail no qual deseja receber as notificações do Amazon SNS.

   Após criar a assinatura, você precisa confirmá-la por meio de seu cliente de e-mail.

Slack setup

Para configurar o Amazon Q Developer em clientes de aplicações de bate-papo – Slack

Depois que você Create an Amazon SNS topic, a próxima etapa é configurar o cliente para o Slack.

Execute as etapas em Tutorial: comece a usar o Slack no Guia do administrador de aplicativos de chat do Amazon Q Developer.

Chime setup

Para configurar o Amazon Q Developer em clientes de aplicações de bate-papo – Chime

Depois que você Create an Amazon SNS topic, a próxima etapa é configurar o Amazon Q Developer para o Chime.

Execute as etapas em Tutorial: comece a usar o Amazon Chime no Guia do administrador de aplicativos de chat do Amazon Q Developer.

Usando a Amazon EventBridge para GuardDuty descobertas

Com EventBridge, você cria regras para especificar os eventos que deseja monitorar. Essas regras também especificam os serviços e aplicações de destino que podem realizar ações automatizadas se esses eventos ocorrerem. Um alvo é um destino (um recurso ou um endpoint) que EventBridge envia um evento para quando o evento corresponde ao padrão de evento definido na regra. Cada evento é um objeto JSON que está em conformidade com o EventBridge esquema dos AWS eventos e contém uma representação JSON de uma descoberta. Você pode personalizar a regra para enviar somente os eventos que atendam a determinados critérios. Para obter mais informações, consulte the section called “Esquema de eventos”. Como os dados das descobertas são estruturados como um EventBridgeevento, você pode monitorar, processar e agir de acordo com as descobertas usando outros aplicativos, serviços e ferramentas.

Para receber notificações sobre GuardDuty descobertas com base em eventos, você deve criar uma EventBridge regra e uma meta para GuardDuty. Essa regra EventBridge permite enviar notificações de descobertas GuardDuty geradas para o alvo especificado na regra.

> **Note**
>
> EventBridge e CloudWatch os eventos são o mesmo serviço e API subjacentes. No entanto, EventBridge inclui recursos adicionais que ajudam você a receber eventos de aplicativos de software como serviço (SaaS) e de seus próprios aplicativos. Como o serviço subjacente e a API são os mesmos, o esquema de eventos para GuardDuty descobertas também é o mesmo.

Como as descobertas arquivadas e não arquivadas funcionam com GuardDuty EventBridge

Para descobertas que você arquiva manualmente, as ocorrências iniciais e todas as ocorrências subsequentes dessas descobertas (geradas após a conclusão do arquivamento) são enviadas EventBridge com base em uma frequência de notificação específica. Para obter mais informações, consulte Entendendo a frequência de EventBridge notificação em GuardDuty.

Para as descobertas que são arquivadas automaticamente comRegras de supressão, as ocorrências iniciais e todas as ocorrências subsequentes dessas descobertas (geradas após a conclusão do arquivamento) não são enviadas para. EventBridge Você pode visualizar essas descobertas arquivadas automaticamente no GuardDuty console.

Esquema de eventos

Um padrão de evento define os dados EventBridge usados para determinar se o evento deve ser enviado ao destino. O EventBridge evento para GuardDuty tem o seguinte formato:

```
{
        "version": "0",
        "id": "cd2d702e-ab31-411b-9344-793ce56b1bc7",
        "detail-type": "GuardDuty Finding",
        "source": "aws.guardduty",
        "account": "111122223333",
        "time": "1970-01-01T00:00:00Z",
        "region": "us-east-1",
        "resources": [],
        "detail": {GUARDDUTY_FINDING_JSON_OBJECT}
```

```
        }
```

O valor `detail` retorna os detalhes do JSON de uma única descoberta como um objeto, em vez de retornar a sintaxe de resposta descobertas inteira que oferece suporte a várias descobertas de uma matriz.

Para obter uma lista completa de todos os parâmetros incluídos`GUARDDUTY_FINDING_JSON_OBJECT`, consulte GetFindings. O parâmetro do `id` que aparece no `GUARDDUTY_FINDING_JSON_OBJECT` é o ID da descoberta descrito anteriormente.

Criação de uma EventBridge regra para GuardDuty descobertas

Os procedimentos a seguir explicam como usar o EventBridge console da Amazon e o AWS Command Line Interface (AWS CLI) para criar uma EventBridge regra para GuardDuty descobertas. A regra detecta EventBridge eventos que usam o esquema e o padrão de eventos para GuardDuty descobertas e envia esses eventos para uma AWS Lambda função para processamento.

AWS Lambda é um serviço de computação que você pode usar para executar código sem provisionar ou gerenciar servidores. Você empacota seu código e o carrega AWS Lambda como uma função Lambda. AWS Lambda em seguida, executa a função quando a função é invocada. Uma função pode ser invocada manualmente por você, automaticamente em resposta a eventos ou em resposta a solicitações de aplicações ou serviços. Para obter mais informações sobre criar e invocar as funções do Lambda, consulte o Guia do desenvolvedor do AWS Lambda.

Escolha seu método preferido para criar uma EventBridge regra que envie sua GuardDuty descoberta para um alvo.

Console

Siga estas etapas para usar o EventBridge console da Amazon para criar uma regra que envia automaticamente todos os eventos de GuardDuty busca para uma função Lambda para processamento. A regra usa configurações padrão para regras que são executadas quando eventos específicos são recebidos. Para obter detalhes sobre as configurações de regras ou para aprender como criar uma regra que usa configurações personalizadas, consulte Criação de regras que reagem a eventos no Guia EventBridge do usuário da Amazon.

Antes de criar essa regra, crie a função do Lambda que deseja que a regra use como destino. Ao criar a regra, você precisará especificar essa função como o destino da regra. Seu destino também pode ser o tópico do SNS criado anteriormente. Para obter mais informações, consulte Configurar um tópico e um endpoint do Amazon SNS (e-mail, Slack e Amazon Chime).

Para criar uma regra de evento usando o console

1. Faça login no Console de gerenciamento da AWS e abra o EventBridge console da Amazon em https://console.aws.amazon.com/events/.
2. No painel de navegação, em Barramentos, selecione Regras.
3. Na seção Regras, selecione Criar regra.
4. Em Definir detalhe da regra, faça o seguinte:

   a. Em Nome, insira um nome para a regra.

   b. (Opcional) Em Descrição, insira uma breve descrição da regra.

   c. Para Barramento de eventos, verifique se o padrão está selecionado e Habilitar a regra nos barramentos de eventos selecionados está ligado.

   d. Para Tipo de regra, escolha Regra com padrão de evento.

   e. Ao terminar, escolha Avançar.
5. Na página Criar padrão de evento, faça o seguinte:

   a. Em Origem do evento, escolha AWS eventos ou eventos de EventBridge parceiros.

   b. (Opcional) Em Exemplo de evento, analise um evento de busca de amostra GuardDuty para saber o que um evento pode conter. Para fazer isso, selecione eventos da AWS . Em seguida, em Eventos de amostra, escolha GuardDutyEncontrar.

   c. Opção 1 - Usando o formulário padrão, um modelo que EventBridge fornece

      Na seção Padrão de evento, faça o seguinte:

      1. Para Método de criação, selecione Usar formulário padrão.
      2. Para Origem do evento, escolha Serviços da AWS.
      3. Para AWS service (Serviço da AWS), escolha GuardDuty.
      4. Em Tipo de evento, escolha GuardDuty Encontrar.

      Ao terminar, escolha Avançar.

   d. Opção 2 – usar padrão de evento personalizado em JSON

      Na seção Padrão de evento, faça o seguinte:

      1. Para Método de criação, selecione Padrão personalizado (editor JSON).

2. Para Padrão de evento, cole o seguinte JSON personalizado que criará um alerta para descobertas médias, altas e críticas. Para obter mais informações, consulte Níveis de gravidade das descobertas.

```
{
  "source": [
    "aws.guardduty"
  ],
  "detail-type": [
    "GuardDuty Finding"
  ],
  "detail": {
    "severity": [
      4,
      4.0,
      4.1,
      4.2,
      4.3,
      4.4,
      4.5,
      4.6,
      4.7,
      4.8,
      4.9,
      5,
      5.0,
      5.1,
      5.2,
      5.3,
      5.4,
      5.5,
      5.6,
      5.7,
      5.8,
      5.9,
      6,
      6.0,
      6.1,
      6.2,
      6.3,
      6.4,
      6.5,
      6.6,
```

```
      6.7,
      6.8,
      6.9,
      7,
      7.0,
      7.1,
      7.2,
      7.3,
      7.4,
      7.5,
      7.6,
      7.7,
      7.8,
      7.9,
      8,
      8.0,
      8.1,
      8.2,
      8.3,
      8.4,
      8.5,
      8.6,
      8.7,
      8.8,
      8.9,
      9,
      9.0,
      9.1,
      9.2,
      9.3,
      9.4,
      9.5,
      9.6,
      9.7,
      9.8,
      9.9,
      10,
      10.0
    ]
  }
}
```

Ao terminar, escolha Avançar.

6. Opção A - Seleção AWS service (Serviço da AWS) - AWS Lambda como alvo

   Na página Selecionar destino(s), faça o seguinte:

   a. Para Tipos de destino, selecione AWS service (Serviço da AWS).

   b. Para Selecionar um destino, escolha Função do Lambda. Em seguida, para Função, selecione a função do Lambda para a qual deseja enviar eventos de descoberta.

   c. version/aliasEm Configurar, insira as configurações de versão ou alias para a função Lambda de destino.

   d. (Opcional) Para Configurações adicionais, insira configurações personalizadas para especificar quais dados de eventos você deseja enviar para a função do Lambda. Você também pode especificar como lidar com eventos que não são entregues à função com sucesso.

   e. Ao terminar, escolha Avançar.

7. Opção B – selecionar tópico do SNS como destino

   Na página Selecionar destino(s), faça o seguinte:

   a. Para Tipos de destino, selecione AWS service (Serviço da AWS).

   b. Em Select a target (Selecionar um destino), escolha SNS topic (Tópico do SNS). Em seguida, para Localização de destino, selecione a opção adequada com base na sua localização de destino. Em Tópico, escolha o nome do tópico do SNS criado.

   c. Expanda Additional settings (Configurações adicionais). Em Configurar entrada do destino, escolha Transformador de entrada.

   d. Escolha Configurar o transformador de entrada.

   e. Copie o código a seguir e cole-o no campo Caminho de entrada na seção Transformador de entrada de destino.

```
{
    "severity": "$.detail.severity",
    "Account_ID": "$.detail.accountId",
    "Finding_ID": "$.detail.id",
    "Finding_Type": "$.detail.type",
    "region": "$.region",
    "Finding_Description": "$.detail.description"
}
```

   f. Copie o código a seguir e cole-o no campo Modelo para formatar o e-mail.

```
{"message":"You have a severity <severity> GuardDuty finding type
 <Finding_Type> in the <region> Region.\n\nFinding Description:
\n<Finding_Description>\n\nFor more details open the GuardDuty console at
 https://console.aws.amazon.com/guardduty/home?region=<region>#/findings?
search=id%3D<Finding_ID>"}
```

Important

Forneça o modelo como um objeto JSON de linha única, com a mensagem encapsulada em uma chave`message`, como mostrado no exemplo anterior. Use \n para adicionar quebras de linha.
GuardDuty campos de busca como os que `description` podem conter caracteres de controle sem escape, incluindo novas linhas. Não use nenhum dos seguintes formatos de modelo:

- Uma string sem aspas
- Um modelo de várias linhas que usa cadeias de caracteres separadas entre aspas em linhas separadas

Com esses formatos, o valor substituído pode produzir JSON inválido. EventBridge em seguida, rejeita o evento e não entrega a notificação.

Note

As assinaturas de e-mail recebem a saída do modelo como está, então o e-mail mostra o objeto `message` JSON e as quebras de linha aparecem como. \n Para notificações formatadas, entregue o tópico do Amazon SNS ao Amazon Q Developer em aplicativos de bate-papo (Slack ou Amazon Chime) ou use uma função Lambda como destino.

8. Na página Configurar tags, insira opcionalmente uma ou mais tags a serem atribuídas à regra. Escolha Próximo.
9. Na página Revisar e criar, analise as configurações da regra e verifique se estão corretas.

Para alterar uma configuração, selecione Editar para a configuração e insira a configuração correta. Você também pode usar as guias de navegação para acessar a página que contém uma configuração.

10. Quando terminar de verificar as configurações, selecione Criar regra.

API

O procedimento a seguir mostra como usar AWS CLI comandos para criar uma EventBridge regra e um destino para GuardDuty. Especificamente, o procedimento mostra como criar uma regra que permite EventBridge enviar eventos para todas as descobertas GuardDuty geradas para uma AWS Lambda função como alvo da regra.

> **Note**
>
> Neste exemplo, estamos usando uma função Lambda como destino para a regra que é acionada. EventBridge Você também pode configurar outros AWS recursos como alvos a serem acionados EventBridge. GuardDuty e EventBridge oferecem suporte aos seguintes tipos de destino: instâncias do Amazon EC2, streams do Amazon Kinesis, tarefas do Amazon ECS, máquinas de estado AWS Step Functions , `run` o comando e destinos integrados. Para obter mais informações, consulte PutTargetsa Amazon EventBridge API Reference.

Para criar uma regra e um destino

1. Para criar uma regra que permita EventBridge enviar eventos para todas as descobertas GuardDuty geradas, execute o seguinte comando da EventBridge CLI.

```
aws events put-rule --name your-rule-name --event-pattern "{\"source\":
[\"aws.guardduty\"]}"
```

Você pode personalizar ainda mais sua regra para que ela EventBridge instrua o envio de eventos somente para um subconjunto das GuardDuty-generated descobertas. Esse subconjunto é baseado no atributo ou nos atributos da descoberta especificado(s) na regra. Por exemplo, use o seguinte comando da CLI para criar uma regra que permite EventBridge enviar somente eventos para as GuardDuty descobertas com a severidade de 5 ou 8:

```
aws events put-rule --name your-rule-name --event-pattern "{\"source\":
[\"aws.guardduty\"],\"detail-type\":[\"GuardDuty Finding\"],\"detail\":
{\"severity\":[5,8]}}"
```

Para isso, você pode usar qualquer um dos valores de propriedade que estão disponíveis no JSON para GuardDuty descobertas.

2. Para anexar uma função Lambda como destino para a regra que você criou na etapa 1, execute o seguinte comando da CLI EventBridge .

```
aws events put-targets --rule your-rule-name --targets
 Id=1,Arn=arn:aws:lambda:us-east-1:111122223333:function:your-function
```

Certifique-se de `your-rule-name` substituir pelo nome da regra que você criou na etapa 1 e `your-function` pela sua função Lambda real para os GuardDuty eventos.

3. Para adicionar as permissões necessárias para invocar o destino, execute o seguinte comando da CLI do Lambda.

```
aws lambda add-permission --function-name your-function --statement-id 1 --
action 'lambda:InvokeFunction' --principal events.amazonaws.com --source-arn
 arn:aws:events:us-east-1:111122223333:rule/your-rule-name
```

Certifique-se de `your-function` substituir os GuardDuty eventos por sua função Lambda real e `your-rule-name` pelo nome da regra que você criou na etapa 1. A `--source-arn` condição permite que somente essa regra invoque a função.

EventBridge regra para ambientes GuardDuty com várias contas

Ao usar uma conta de GuardDuty administrador delegado, você pode visualizar os eventos gerados nas contas dos membros e agir usando outros aplicativos e serviços. EventBridge as regras em sua conta de administrador serão acionadas com base nas descobertas aplicáveis de suas contas de membros. Se você configurar notificações de busca por meio EventBridge de sua conta de administrador, receberá notificações de descobertas tanto da sua conta quanto das contas dos membros. Por exemplo, você pode usar EventBridge para enviar tipos específicos de descobertas para uma função Lambda que processa e envia os dados para seu sistema de gerenciamento de incidentes e eventos de segurança (SIEM).

Você pode identificar a conta do membro de onde a GuardDuty descoberta se originou usando o `accountId` campo dos detalhes JSON da descoberta. Para criar uma regra de evento personalizada para contas de membros específicas, crie uma nova regra e use o modelo a seguir em Padrão de eventos. *123456789012*Substitua pela conta `accountId` do membro para a qual você deseja acionar o evento.

```
{
  "source": [
    "aws.guardduty"
  ],
  "detail-type": [
    "GuardDuty Finding"
  ],
  "detail": {
    "accountId": [
      "123456789012"
    ]
  }
}
```

> **Note**
>
> Esse exemplo cria uma regra que corresponde a todas as descobertas do ID da conta especificada. Você pode incluir vários IDs de conta separando-os com vírgulas, seguindo a sintaxe JSON.

Entendendo CloudWatch os registros e os motivos para pular recursos durante a verificação do Malware Protection for EC2

GuardDuty O Malware Protection for EC2 publica eventos em seu grupo de CloudWatch log da Amazon//aws/guardduty/malware-scan-events. Para cada um dos eventos relacionados à verificação de malware, é possível monitorar o status e o resultado da verificação dos recursos afetados. Alguns recursos do Amazon EC2 e volumes do Amazon EBS podem ter sido ignorados durante a Proteção contra malware para a verificação EC2.

CloudWatch Registros de auditoria na proteção contra GuardDuty malware para EC2

Há três tipos de eventos de escaneamento suportados no grupo de log/aws/guardduty CloudWatch / malware-scan-events.

Nome do evento de verificação da Proteção contra malware para EC2	Explicação
`EC2_SCAN_STARTED`	Criado quando uma proteção contra GuardDuty malware para EC2 está iniciando o processo de verificação de malware, como se preparando para tirar um instantâneo de um volume do EBS.
`EC2_SCAN_COMPLETED`	Criado quando a verificação do GuardDuty Malware Protection for EC2 é concluída em pelo menos um dos volumes do EBS do recurso afetado. Esse evento também inclui o `snapshotId` pertencente ao volume do EBS verificado. Após a conclusão da verificação, o resultado da verificação será `CLEAN`, `THREATS_FOUND` ou `NOT_SCANNED` .
`EC2_SCAN_SKIPPED`	Criado quando a verificação do GuardDuty Malware Protection for EC2 ignora todos os volumes do EBS do recurso afetado. Para identificar porque foram ignorados, selecione o evento correspondente e veja os detalhes. Para obter mais informações sobre os motivos para ignorar, veja Razões para ignorar o recurso durante a verificação de malware abaixo.

> **Note**
>
> Se você estiver usando um AWS Organizations, os eventos de CloudWatch registro das contas dos membros nas Organizações serão publicados na conta do administrador e no grupo de registro da conta do membro.

Escolha seu método de acesso preferido para visualizar e consultar CloudWatch eventos.

Console

1. Faça login no Console de gerenciamento da AWS e abra o CloudWatch console em https://console.aws.amazon.com/cloudwatch/.
2. No painel de navegação, em Logs, escolha Grupos de logs. Escolha o grupo de log/aws/guardduty/malware-scan-events para visualizar os eventos de verificação do Malware Protection for EC2. GuardDuty

   Para executar uma consulta, escolha Log Insights.

   Para obter informações sobre como executar uma consulta, consulte Análise de dados de log com o CloudWatch Logs Insights no Guia CloudWatch do usuário da Amazon.
3. Escolha ID de verificação para monitorar os detalhes do recurso afetado e as descobertas do malware. Por exemplo, você pode executar a consulta a seguir para filtrar os eventos de CloudWatch log usando`scanId`. Certifique-se de usar o seu próprio válido*`scan-id`*.

   ```
   fields @timestamp, @message, scanRequestDetails.scanId as scanId
   | filter scanId like "77a6f6115da4bd95f4e4ca398492bcc0"
   | sort @timestamp asc
   ```

API/CLI

- Para trabalhar com grupos de registros, consulte Pesquisar entradas de registro usando o AWS CLI no Guia CloudWatch do usuário da Amazon.

  Escolha o grupo de log/aws/guardduty/malware-scan-events para visualizar os eventos de verificação do Malware Protection for EC2. GuardDuty
- Para visualizar e filtrar eventos de log, consulte GetLogEvents e FilterLogEvents, respectivamente, na Referência de CloudWatch API da Amazon.

GuardDuty Proteção contra malware para retenção de registros do EC2

O período padrão de retenção de registros para o grupo de registros/aws/guardduty/malware-scan-events é de 90 dias, após os quais os eventos de log são excluídos automaticamente. Para alterar a política de retenção de logs do seu CloudWatch grupo de CloudWatch logs, consulte Alterar a retenção de dados de log em Logs no Guia CloudWatch do usuário da Amazon ou PutRetentionPolicy na Amazon CloudWatch API Reference.

Razões para ignorar o recurso durante a verificação de malware

Nos eventos relacionados à verificação de malware, alguns recursos do EC2 e volumes do EBS podem ter sido ignorados durante o processo de verificação. A tabela a seguir lista os motivos pelos quais o GuardDuty Malware Protection for EC2 pode não escanear os recursos. Se aplicável, use as etapas propostas para resolver esses problemas e verifique esses recursos na próxima vez que o GuardDuty Malware Protection for EC2 iniciar uma verificação de malware. Os outros problemas são usados para informar você sobre o curso dos eventos e não são acionáveis.

Razões para ignorar	Explicação	Etapas propostas
`RESOURCE_NOT_FOUND`	O `resourceArn` fornecido para iniciar a verificação de malware sob demanda não foi encontrado em seu AWS ambiente.	Valide a `resourceArn` de sua instância do Amazon EC2 ou workload de contêiner e tente novamente.
`ACCOUNT_INELIGIBLE`	A ID da AWS conta a partir da qual você tentou iniciar uma verificação de On-demand malware não foi ativada GuardDuty.	Verifique se GuardDuty está habilitado para essa AWS conta. Quando você ativa GuardDuty em um novo Região da AWS , pode levar até 20 minutos para sincronizar.

Razões para ignorar	Explicação	Etapas propostas	
`UNSUPPORTED_KEY_ENCRYPTION`	GuardDuty O Malware Protection for EC2 oferece suporte a volumes não criptografados e criptografados com a chave gerenciada pelo cliente. Ele não suporta a verificação de volumes do EBS que são criptografados usando a criptografia do Amazon EBS. Atualmente, há uma diferença regional em que esse motivo de salto não é aplicável. Para obter mais informações sobre eles Regiões da AWS, consulte Region-specific disponibilidade de recursos.	Substitua a chave de criptografia por uma chave gerenciada pelo cliente. Para obter mais informações sobre os tipos de criptografia GuardDuty compatíveis, consulte Volumes Amazon EBS compatíveis para verificação de malware.	

Razões para ignorar	Explicação	Etapas propostas	
`EXCLUDED_BY_SCAN_SETTINGS`	Durante a verificação de malware, a instância do EC2 ou o volume do EBS foi excluído. Há três possibilidades: a tag foi adicionada à lista de inclusão, mas o recurso não está associado a essa tag; a tag foi adicionada à lista de exclusão e o recurso está associado a essa tag; ou a tag `GuardDutyExcluded` está definida como `true` para esse recurso.	Atualize suas opções de verificação ou as tags associadas ao seu recurso do Amazon EC2. Para obter mais informações, consulte Opções de verificação com tags definidas pelo usuário.	
`UNSUPPORTED_VOLUME_SIZE`	O volume é maior que 2048 GB.	Não acionável.	
`NO_VOLUMES_ATTACHED`	GuardDuty O Malware Protection for EC2 encontrou a instância em sua conta, mas nenhum volume do EBS foi anexado a essa instância para continuar com a verificação.	Não acionável.	
`UNABLE_TO_SCAN`	É um erro de serviço interno.	Não acionável.	

Razões para ignorar	Explicação	Etapas propostas	
SNAPSHOT_NOT_FOUND	Os instantâneos criados a partir dos volumes do EBS e compartilhados com a conta de serviço não foram encontrados, e o GuardDuty Malware Protection for EC2 não pôde continuar com a verificação.	Verifique CloudTrail se os instantâneos não foram removidos intencionalmente.	
SNAPSHOT_QUOTA_REACHED	Você atingiu o volume máximo permitido para snapshots em cada região. Isso evita não apenas reter, mas também criar novos snapshots.	Você pode remover snapshots antigos ou solicitar o aumento da cota. Você pode ver o limite padrão para snapshots por região e como solicitar o aumento da cota em Cotas de serviço no Guia de referência geral da AWS .	
MAX_NUMBER_OF_ATTACHED_VOLUMES_REACHED	Mais de 11 volumes do EBS foram anexados a uma instância do EC2. GuardDuty O Malware Protection for EC2 verificou os primeiros 11 volumes do EBS, obtidos classificando-os em ordem alfabética. deviceName	Não acionável.	

Razões para ignorar	Explicação	Etapas propostas	
`UNSUPPORTED_PRODUCT_CODE_TYPE`	GuardDuty pode escanear a maioria das instâncias com `productCode` as`marketplace` . Algumas instâncias do marketplace podem não estar qualificadas para escaneamento. GuardDuty ignorará essas instâncias e registrará o motivo como`UNSUPPORTED_PRODUCT_CODE_TYPE` . Esse suporte varia nas regiões da China e AWS GovCloud (US) . Para obter mais informações, consulte Region-specific disponibilidade de recursos. Para mais informações, consulte AMIs pagas no Guia do usuário do Amazon EC2 para instâncias do Linux. Para obter mais informações, consulte `productCode` Ações de ProductCode na	Não acionável.	

Razões para ignorar	Explicação	Etapas propostas	
	Referência da API do Amazon EC2.		

Denunciando falsos positivos na Proteção contra malware para EC2

GuardDuty A proteção contra malware para escaneamentos do EC2 pode identificar um arquivo inofensivo na sua instância ou carga de trabalho do contêiner do Amazon EC2 como sendo malicioso ou prejudicial. Para melhorar sua experiência com o Malware Protection for EC2 e o GuardDuty serviço, você pode denunciar resultados falsos positivos se acreditar que um arquivo identificado como malicioso ou prejudicial durante uma verificação não contém realmente malware.

Para denunciar resultado falso positivo na verificação de malware para Amazon EC2 como falso positivo

Para iniciar o processo, entre em contato com Suporte. Use as etapas a seguir para fornecer detalhes sobre o recurso escaneado:

1. Faça login no Console de gerenciamento da AWS e abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.
2. Selecione Verificações de malware para EC2.
3. Escolha um verificação para ver seu ID de descoberta.
4. Forneça o ID de descoberta. Você também deve fornecer o SHA-256 hash do arquivo. Isso é necessário para garantir que o GuardDuty Malware Protection for EC2 tenha recebido o arquivo correto.
5. A Suporte equipe fornecerá a você uma URL pré-assinada do Amazon Simple Storage Service (Amazon S3) que você poderá usar para carregar o arquivo e o hash potencialmente maliciosos. SHA-256 Para obter informações sobre as etapas para fazer o upload do objeto verificado, consulte Carregamento de objetos com URLs pré-assinados no Guia do usuário do Amazon S3.
6. Depois de fazer o upload do arquivo, informe a Suporte equipe.

   Eles Suporte fornecerão uma confirmação após o recebimento do arquivo. Os membros da equipe de GuardDuty serviço analisarão seu envio e tomarão as medidas apropriadas para melhorar sua experiência com o Malware Protection for EC2 e o GuardDuty serviço. A Suporte

equipe continuará fornecendo atualizações sobre o status do seu caso. GuardDuty mantém seu objeto S3 por no máximo 30 dias.

Relatar o resultado da verificação de objetos do S3 como falso positivo na Proteção contra Malware do S3

Uma verificação da Proteção contra Malware para S3 pode identificar um objeto como potencialmente malicioso ou prejudicial. Se você acredita que o objeto S3 indicado não contém malware, relate esse resultado da verificação de malware como um falso positivo.

Você pode enviar uma denúncia de falso positivo mesmo usando a Proteção contra Malware para S3 de forma independente. Nesse caso, GuardDuty não foi projetado para gerar uma descoberta. Para obter informações sobre como verificar o status de verificação e o status do resultado, consulteMonitoramento de verificações de objetos de S3.

Para denunciar resultado falso positivo na verificação de malware S3 como falso positivo

Para iniciar o processo, entre em contato com Suporte. Siga as etapas abaixo para fornecer detalhes sobre o objeto S3 verificado:

1. Faça login no Console de gerenciamento da AWS e abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.
2. Dependendo do seu caso de uso, escolha as etapas apropriadas:

   Using Malware Protection for S3 with GuardDuty

   1. No painel de navegação, selecione Descobertas.
   2. Na página Descobertas, selecione a descoberta de falso positivo para ver seus detalhes.
   3. Ao verificar os detalhes da descoberta, forneça a ID da descoberta, a região, o nome do bucket S3 protegido e a chave do objeto verificado.

      Nos detalhes do caminho do item, forneça o Hash do objeto. Isso é necessário para garantir que GuardDuty recebeu o arquivo correto.

   Using Malware Protection for S3 independently

   Forneça o nome do bucket S3 protegido, o nome do objeto verificado e Região da AWS.

3. A Suporte equipe fornecerá uma URL pré-assinada do Amazon Simple Storage Service (Amazon S3) que você poderá usar para carregar o arquivo e o hash potencialmente maliciosos. Para obter informações sobre as etapas para fazer o upload do objeto verificado, consulte Carregamento de objetos com URLs pré-assinados no Guia do usuário do Amazon S3.
4. Depois de fazer o upload do objeto S3, informe a Suporte equipe.

Eles Suporte fornecerão uma confirmação de recebimento do objeto. Os membros da equipe de GuardDuty serviço analisarão seu envio e tomarão as medidas apropriadas para melhorar sua experiência com o Malware Protection for S3 e o GuardDuty serviço. A Suporte equipe continuará fornecendo atualizações sobre o status do seu caso. GuardDuty mantém seu objeto S3 por no máximo 30 dias.

Denunciando falsos positivos no Malware Protection for Backup

Para melhorar sua experiência com o GuardDuty Malware Protection for Backup, você pode denunciar possíveis falsos positivos e falsos negativos.

Para denunciar um potencial falso positivo ou falso negativo identificado no Malware Protection for Backup

Para iniciar o processo, entre em contato com Suporte. Use as etapas a seguir para fornecer detalhes sobre o recurso digitalizado:

1. Faça login no Console de gerenciamento da AWS e abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.
2. Selecione Verificações de malware.
3. Escolha um verificação para ver seu ID de busca.
4. Forneça o ID de descoberta. Você também deve fornecer o SHA-256 hash do arquivo. Isso é necessário para garantir que GuardDuty recebeu o arquivo correto. Forneça também a região da qual você fornecerá a amostra.
5. A Suporte equipe fornecerá uma URL pré-assinada do Amazon Simple Storage Service (Amazon S3) que você usará para carregar o arquivo e o hash potencialmente maliciosos. SHA-256 Para obter informações sobre as etapas para carregar o recurso digitalizado, consulte Carregamento de objetos com URLs pré-assinados no Guia do usuário do Amazon S3.
6. Depois de fazer o upload do arquivo, informe a Suporte equipe.

Eles Suporte fornecerão uma confirmação após o recebimento do arquivo. Os membros da equipe de GuardDuty serviço analisarão seu envio e tomarão as medidas apropriadas para melhorar sua experiência com o Malware Protection for EC2. A Suporte equipe continuará fornecendo atualizações de status sobre seu caso. GuardDuty mantém seu objeto S3 por no máximo 30 dias.

Corrigindo descobertas de GuardDuty segurança detectadas

GuardDuty A Amazon gera descobertas que indicam possíveis descobertas de segurança associadas à detecção GuardDuty básica de ameaças e a planos de proteção dedicados. As seções a seguir descrevem as etapas de correção recomendadas para qualquer uma das situações. Caso ocorram cenários alternativos de correção, eles serão descritos nas descrições para cada tipo de descoberta. Para acessar as informações completas sobre um tipo de descoberta selecione-a na tabela Tipos de descobertas ativas.

Conteúdo

- Como corrigir uma instância do Amazon EC2 potencialmente comprometida
- Como corrigir um bucket do S3 possivelmente comprometido
- Como corrigir um objeto do S3 possivelmente malicioso
- Corrigindo um snapshot do EBS potencialmente comprometido
- Corrigindo uma AMI do EC2 potencialmente comprometida
- Corrigindo um ponto de recuperação EC2 potencialmente comprometido
- Corrigindo um ponto de recuperação S3 potencialmente comprometido
- Como corrigir um cluster do ECS possivelmente comprometido
- Correção de problemas potencialmente comprometidos AWS credenciais
- Como corrigir um contêiner autônomo possivelmente comprometido
- Como corrigir as descobertas da Proteção do EKS
- Como corrigir as descobertas do Monitoramento de runtime
- Corrigir um banco de dados possivelmente comprometido
- Correção de uma função do Lambda comprometida

Como corrigir uma instância do Amazon EC2 potencialmente comprometida

Quando GuardDuty gera tipos de descoberta que indicam recursos do Amazon EC2 potencialmente comprometidos, seu recurso será Instância. Os possíveis tipos de descoberta podem serTipos de descoberta do EC2,GuardDuty Tipos de descoberta de monitoramento de tempo de execução, ou

Tipos de descoberta da Proteção contra malware para EC2. Caso o comportamento que causou a descoberta seja esperado em seu ambiente, considere usar o Regras de supressão.

Execute as seguintes etapas para corrigir a instância possivelmente comprometida do Amazon EC2:

1. Identifique a instância possivelmente comprometida do Amazon EC2

   Verifique se há malwares na instância possivelmente comprometida e remova todos aqueles que forem descobertos. Use a On-demand escaneamento de malware em GuardDuty para identificar um malware na instância EC2 possivelmente comprometida ou verifique o AWS Marketplace para conferir se há produtos parceiros úteis para identificar e remover malware.

2. Isole a instância possivelmente comprometida do Amazon EC2

   Se possível, use as etapas a seguir para isolar a instância possivelmente comprometida:

   1. Crie um grupo de segurança de isolamento específico. Um grupo de segurança de isolamento só deve ter acesso para entrada e saída de endereços IP específicos. Certifique-se de que não haja nenhuma regra de entrada ou saída que permita o tráfego para `0.0.0.0/0 (0-65535)`.
   2. Associe o grupo de segurança Isolamento a essa instância.
   3. Remova todas as associações de grupos de segurança, exceto o recém-criado grupo de segurança Isolamento, da instância possivelmente comprometida.

   > **Note**
   >
   > As conexões rastreadas existentes não serão encerradas como resultado da alteração dos grupos de segurança - somente o tráfego futuro será efetivamente bloqueado pelo novo grupo de segurança.
   > Para obter informações sobre como bloquear mais tráfego de conexões suspeitas existentes, consulte Aplicar NACLs com base na rede IoCs para evitar mais tráfego no Manual de resposta a incidentes.

3. Identifique a origem da atividade suspeita

   Se for detectado um malware, com base no tipo de descoberta em sua conta, identifique e interrompa a atividade potencialmente não autorizada em sua instância do EC2. Isso pode exigir medidas como fechar todas as portas abertas, alterar as políticas de acesso e atualizar aplicações para corrigir as vulnerabilidades.

Caso não consiga identificar e interromper atividades não autorizadas em sua instância do EC2 possivelmente comprometida, recomendamos encerrar a instância do EC2 comprometida e substituí-la por uma nova instância, caso necessário. Veja a seguir os recursos adicionais para proteger suas instâncias do EC2:

- Seções Segurança e Rede em Melhores práticas do Amazon EC2.
- Grupos de segurança do Amazon EC2 para instâncias do Linux.
- Segurança no Amazon EC2
- Dicas para proteger as instâncias do EC2 (Linux).
- AWS melhores práticas de segurança
- AWS Guia técnico de resposta a incidentes de segurança.

4. Navegar AWS re:Post

   Navegue AWS re:Postpara obter mais assistência.

5. Envie uma solicitação de suporte técnico

   Caso seja assinante do pacote Premium Support, envie uma solicitação de suporte técnico.

Como corrigir um bucket do S3 possivelmente comprometido

Quando GuardDuty geradoGuardDuty Tipos de localização do S3 Protection, indica que seus buckets do Amazon S3 foram comprometidos. Caso o comportamento que causou a descoberta fosse esperado em seu ambiente, considere criarRegras de supressão. Se esse comportamento não fosse esperado, siga estas etapas recomendadas para remediar um bucket do Amazon S3 potencialmente comprometido em seu ambiente: AWS

1. Identifique o recurso do S3 possivelmente comprometido.

   Uma GuardDuty descoberta para o S3 listará o bucket do S3 associado, seu nome de recurso da Amazon (ARN) e seu proprietário nos detalhes da descoberta.

2. Identifique a origem da atividade suspeita e a chamada de API usada.

   A chamada de API usada será listada como `API` nos detalhes da descoberta. A origem será uma entidade principal do IAM (um perfil, um usuário ou uma conta do IAM) e os detalhes de identificação serão listados na descoberta. Dependendo do tipo de origem, o endereço IP remoto ou as informações do domínio de origem estarão disponíveis e poderão ajudar a avaliar se a

origem foi autorizada. Caso a descoberta envolva credenciais de uma instância do Amazon EC2, os detalhes desse recurso também serão incluídos.

3. Determine se a origem da chamada foi autorizada a acessar o recurso identificado.

   Por exemplo, considere o seguinte:

   - Caso um usuário do IAM esteja envolvido, é possível que suas credenciais tenham sido possivelmente comprometidas? Para obter mais informações, consulte Correção de problemas potencialmente comprometidos AWS credenciais.
   - Caso uma API tenha sido invocada a partir de uma entidade principal que não tenha histórico anterior de invocação desse tipo de API, essa fonte precisa de permissões de acesso para essa operação? É possível restringir ainda mais as permissões do bucket?
   - Se o acesso foi visto a partir do nome de usuário `ANONYMOUS_PRINCIPAL` com o tipo de usuário `AWSAccount`, isso indica que o bucket é público e foi acessado. Esse bucket deveria ser público? Se a resposta for não, revise as recomendações de segurança abaixo a fim de encontrar soluções alternativas para compartilhar recursos do S3.
   - Se o acesso foi feito por meio de uma chamada `PreflightRequest` bem-sucedida vista do nome de usuário `ANONYMOUS_PRINCIPAL` com o tipo de usuário `AWSAccount`, isso indica que o bucket tem uma política de compartilhamento de recursos de origem cruzada (CORS) definida. Esse bucket deve ter uma política de CORS? Se a resposta for não, certifique-se de que o bucket não esteja designado como público por engano e analise as recomendações de segurança abaixo a fim de encontrar soluções alternativas para compartilhar recursos do S3. Para obter mais informações sobre o CORS, consulte Usar o compartilhamento de recursos de origem cruzada (CORS) no guia do usuário do S3.

4. Determine se o bucket do S3 contém dados confidenciais.

   Use o Amazon Macie para determinar se o bucket do S3 contém dados confidenciais, como informações de identificação pessoal (PII), dados financeiros ou credenciais. Se a descoberta automatizada de dados confidenciais estiver habilitada para sua conta do Macie, revise os detalhes do bucket do S3 a fim de entender melhor o conteúdo do bucket do S3. Se esse atributo estiver desabilitado em sua conta do Macie, recomendamos habilitá-lo para agilizar sua avaliação. Outra alternativa é criar e executar um trabalho de descoberta de dados confidenciais para inspecionar os objetos do bucket do S3 em busca de dados confidenciais. Para obter mais informações, consulte Discovering sensitive data with Amazon Macie.

A descoberta pode ser ignorada se o acesso foi autorizado. O https://console.aws.amazon.com/guardduty/ console permite que você configure regras para suprimir totalmente as descobertas

individuais para que elas não apareçam mais. Para obter mais informações, consulte Regras de supressão em GuardDuty.

Ao determinar que seus dados do S3 foram expostos ou acessados por uma parte não autorizada, analise as seguintes recomendações de segurança do S3 para reforçar as permissões e restringir o acesso. As soluções de correção apropriadas serão determinadas pelas necessidades de seu ambiente específico.

Recomendações com base em necessidades específicas de acesso a buckets do S3

A lista a seguir fornece recomendações com base nas necessidades específicas de acesso ao bucket do Amazon S3:

- Para limitar o acesso público ao uso de dados do S3 de forma centralizada, bloqueie o acesso público do S3. As configurações de bloqueio de acesso público podem ser habilitadas para pontos de acesso, buckets e AWS contas por meio de quatro configurações diferentes para controlar a granularidade do acesso. Para obter mais informações, consulte Bloquear configurações de acesso público no Guia do usuário do Amazon S3.
- AWS As políticas de acesso podem ser usadas para controlar como os usuários do IAM podem acessar seus recursos ou como seus buckets podem ser acessados. Para obter mais informações, consulte Usar políticas de bucket e políticas de usuário no Guia do usuário do Amazon S3.

  Além disso, você pode usar endpoints da nuvem privada virtual (VPC) com políticas de bucket do S3 para restringir o acesso a endpoints da VPC específicos. Para obter mais informações, consulte Controlar o acesso a partir de endpoints da VPC com políticas de bucket no Guia do usuário do Amazon S3.
- Para permitir que entidades confiáveis fora de sua conta acessem temporariamente os objetos do S3, é possível criar um URL pré-assinado por meio do S3. Esse acesso é criado com as credenciais da sua conta e, dependendo das credenciais usadas, pode durar de 6 horas a 7 dias. Para obter mais informações, consulte Usar URLs pré-assinados para baixar e fazer upload de objetos no Guia do Usuário do Amazon S3.
- Para os casos de uso que exigem o compartilhamento de objetos do S3 entre diferentes origens, use os Pontos de Acesso S3 para criar conjuntos de permissões que restringem o acesso somente aos que estão em sua rede privada. Para obter mais informações, consulte Gerenciar o acesso a conjunto de dados compartilhados com pontos de acesso no Guia do usuário do Amazon S3.

- Para conceder acesso seguro aos seus recursos do S3 para outras AWS contas, você pode usar uma lista de controle de acesso (ACL). Para obter mais informações, consulte a visão geral da lista de controle de acesso (ACL) no Guia do usuário do Amazon S3.

Para obter mais informações sobre as opções de segurança do S3, consulte Práticas recomendadas de segurança para o Amazon S3 no Guia do usuário do Amazon S3.

Como corrigir um objeto do S3 possivelmente malicioso

Quando GuardDuty geradoTipo de descoberta da Proteção contra malware para S3, indica que um objeto recém-carregado em seu bucket do Amazon S3 contém malware. O tipo de recurso é um S3Object.

Use as seguintes etapas recomendadas para corrigir a descoberta gerada:

1. Identifique o objeto S3 potencialmente malicioso verificando o S3ObjectDetails associado à descoberta.
2. Isole o objeto do S3 afetado. Se você habilitou a marcação no momento da ativação da Proteção contra Malware para S3 para o bucket associado do Amazon S3, GuardDuty deve ter atribuído uma tag maliciosa a esse objeto. Use o controle de acesso baseado em tags (TBAC) para restringir o acesso a esse objeto do S3. Para obter mais informações, consulte Usando controle de acesso baseado em tags (TBAC).

   Outra alternativa é que, caso não precise mais desse objeto, também é possível optar por excluí-lo ou movê-lo para um bucket do S3 isolado. Para obter informações sobre considerações para a exclusão de um objeto do S3, consulte Exclusão de objetos no Guia do usuário do Amazon S3.

Corrigindo um snapshot do EBS potencialmente comprometido

Quando GuardDuty gera um Execution:EC2/MaliciousFile! Tipo de localização de snapshot, indica que um malware foi detectado em um snapshot do Amazon EBS. Execute as etapas a seguir para corrigir o snapshot potencialmente comprometido:

1. Identifique o instantâneo potencialmente comprometido

   1. Identifique o instantâneo potencialmente comprometido. A GuardDuty descoberta de um snapshot do EBS listará o ID do snapshot afetado, seu Amazon Resource Name (ARN) e os detalhes associados à verificação de malware nos detalhes da descoberta.

2. Analise os detalhes do ponto de recuperação usando o seguinte comando:

```
aws backup describe-recovery-point –backup-vault-name 021345abcdef6789 –recovery-point-arn "arn:aws:ec2:us-east-1::snapshot/snap-abcdef01234567890"
```

2. Restrinja o acesso ao instantâneo comprometido

   Analise e modifique as políticas de acesso ao cofre de backup para restringir o acesso aos pontos de recuperação e suspender qualquer trabalho de restauração automatizado que possa usar esse instantâneo.

   1. Revise as permissões de compartilhamento atuais:

```
aws ec2 describe-snapshot-attribute --snapshot-id snap-abcdef01234567890 --attribute createVolumePermission
```

   2. Remova o acesso específico à conta:

```
aws ec2 modify-snapshot-attribute --snapshot-id snap-abcdef01234567890 --attribute createVolumePermission --operation-type remove --user-ids 111122223333
```

   3. Para obter opções adicionais da CLI, consulte a documentação da CLI modify-snapshot-attribute.

3. Tome medidas de remediação

   - Antes de prosseguir com a exclusão, certifique-se de ter identificado todas as dependências e de ter backups adequados, se necessário.

Corrigindo uma AMI do EC2 potencialmente comprometida

Quando GuardDuty gera um Execution:EC2/MaliciousFile! Tipo de descoberta de AMI, indica que um malware foi detectado em uma Amazon Machine Image (AMI). Execute as etapas a seguir para corrigir a AMI potencialmente comprometida:

1. Identifique a AMI potencialmente comprometida

   1. Uma GuardDuty descoberta de AMIs listará o ID da AMI afetada, seu nome de recurso da Amazon (ARN) e os detalhes associados à verificação de malware nos detalhes da descoberta.

2. Revise a imagem de origem da AMI:

```
aws ec2 describe-images --image-ids ami-021345abcdef6789
```

2. Restrinja o acesso aos recursos comprometidos

1. Analise e modifique as políticas de acesso ao cofre de backup para restringir o acesso ao ponto de recuperação e suspender qualquer trabalho de restauração automatizado que possa usar esse ponto de recuperação.
2. Remover permissões das permissões da AMI de origem

   Visualize primeiro as permissões existentes:

```
aws ec2 describe-image-attribute --image-id ami-abcdef01234567890 --attribute
 launchPermission
```

   Em seguida, remova as permissões individuais:

```
aws ec2 modify-image-attribute --image-id ami-abcdef01234567890 --launch-
permission '{"Remove":[{"UserId":"111122223333"}]}'
```

   Para opções adicionais de CLI, consulte Compartilhar uma AMI com contas específicas - Amazon Elastic Compute Cloud
3. Se a origem for uma instância do EC2, consulte: Remediando uma instância do Amazon EC2 potencialmente comprometida.

3. Tome medidas de remediação

- Antes de prosseguir com a exclusão, certifique-se de ter identificado todas as dependências e de ter backups adequados, se necessário.

Corrigindo um ponto de recuperação EC2 potencialmente comprometido

Quando GuardDuty gera um Execution:EC2/MaliciousFile! RecoveryPoint tipo de localização, indica que um malware foi detectado em um recurso de backup do EC2 Recovery Point. Execute as etapas a seguir para corrigir o ponto de recuperação potencialmente comprometido:

1. Identifique o ponto de recuperação do EC2 potencialmente comprometido

    1. Uma GuardDuty descoberta do EC2 Recovery Point listará seu Amazon Resource Name (ARN) e os detalhes associados à verificação de malware nos detalhes da descoberta:

    ```
    aws backup describe-recovery-point --backup-vault-name 021345abcdef6789
     --recovery-point-arn "arn:aws:backup:us-east-1:111122223333:recovery-
    point:a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
    ```

    2. Analise os detalhes da recuperação para procurar a imagem de origem:

    ```
    aws backup get-recovery-point-restore-metadata --backup-vault-
    name 021345abcdef6789 --recovery-point-arn "arn:aws:backup:us-
    east-1:111122223333:recovery-point:a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
    ```

2. Restrinja o acesso aos recursos comprometidos

    - Analise e modifique as políticas de acesso ao cofre de backup para restringir o acesso ao ponto de recuperação e suspender qualquer trabalho de restauração automatizado que possa usar esse ponto de recuperação. Se seu ambiente usa marcação de recursos, marque o ponto de recuperação adequadamente para indicar que ele está sob investigação e considere pausar os backups agendados, se necessário.

      Exemplo:

      ```
      aws backup tag-resource --resource-arn arn:aws:backup:us-
      east-1:111122223333:recovery-point:a1b2c3d4-5678-90ab-cdef-
      EXAMPLE11111 --tags Investigation=Malware,DoNotDelete=True
      ```

3. Tome medidas de remediação

    - Antes de prosseguir com a exclusão, certifique-se de ter identificado todas as dependências e de ter backups adequados, se necessário.

Corrigindo um ponto de recuperação S3 potencialmente comprometido

Quando GuardDuty gera um Execution:S3/MaliciousFile! RecoveryPoint tipo de descoberta, indica que um malware foi detectado em um recurso de backup do S3 Recovery Point. Execute as etapas a seguir para corrigir o ponto de recuperação potencialmente comprometido:

1. Identifique o ponto de recuperação S3 potencialmente comprometido

    1. Uma GuardDuty descoberta dos pontos de recuperação do S3 listará o ARN do ponto de recuperação afetado, o nome do cofre de backup e os detalhes associados à verificação de malware nos detalhes da descoberta.
    2. Analise os detalhes do ponto de recuperação:

    ```
    aws backup describe-recovery-point --backup-vault-name 021345abcdef6789
     --recovery-point-arn arn:aws:backup:us-east-1:123456789012:recovery-
    point:abcdef01234567890
    ```

2. Restrinja o acesso aos recursos comprometidos

    - Analise e modifique as políticas de acesso ao cofre de backup para restringir o acesso ao ponto de recuperação e suspender qualquer trabalho de restauração automatizado que possa usar esse ponto de recuperação. Se seu ambiente usa marcação de recursos, marque o ponto de recuperação adequadamente para indicar que ele está sob investigação e considere pausar os backups agendados, se necessário.

      Exemplo:

      ```
      aws backup tag-resource –resource-arn arn:aws:backup:us-
      east-1:111122223333:recovery-point:abcdef01234567890 –
      tags Investigation=Malware,DoNotDelete=True
      ```

      Para obter detalhes adicionais, consulte: Referência de comandos da CLI tag-resource

3. Tome medidas de remediação

    - Antes de prosseguir com a exclusão, certifique-se de ter identificado todas as dependências e de ter backups adequados, se necessário.

Como corrigir um cluster do ECS possivelmente comprometido

Uma descoberta de cluster ECS potencialmente comprometido indica que uma atividade suspeita ou maliciosa foi detectada em seu ambiente Amazon ECS. Isso pode incluir acesso não autorizado, execução de malware ou outro comportamento malicioso que coloque em risco as cargas de trabalho do contêiner.

Siga estas etapas para remediar um cluster do Amazon ECS potencialmente comprometido:

1. Identifique o cluster ECS potencialmente comprometido e a ameaça detectada (descobertas)

   Os detalhes do cluster ECS afetado estão listados no painel de detalhes da GuardDuty descoberta.

2. Avalie a fonte de threat/malware

   Verifique se há malware nas imagens do contêiner. Se um malware for detectado, revise a imagem do contêiner que está sendo usada. Use ListTasks para identificar todas as outras tarefas em execução que usam a mesma imagem potencialmente comprometida.

3. Isole as tarefas afetadas

   Pare a ameaça bloqueando todo o tráfego de rede (tanto de entrada quanto de saída) para as tarefas afetadas. Esse isolamento de rede ajuda a evitar ataques contínuos ao cortar todas as conexões com a tarefa comprometida.

Nota: Se você determinar que essa descoberta foi acionada pela expected/legitimate atividade em seu ambiente, você pode configurar uma regra de supressão para evitar que descobertas semelhantes apareçam. Para obter informações adicionais, consulte Regras de supressão em GuardDuty.

Correção de problemas potencialmente comprometidos AWS credenciais

Quando GuardDuty geradoTipos de descobertas do IAM, indica que suas AWS credenciais foram comprometidas. O tipo de recurso potencialmente comprometido é AccessKey.

Para corrigir credenciais potencialmente comprometidas em seu AWS ambiente, execute as seguintes etapas:

1. Identifique a entidade do IAM possivelmente comprometida e a chamada de API usada.

   A chamada de API usada será listada como `API` nos detalhes da descoberta. A entidade do IAM (um usuário ou um perfil do IAM) e as respectivas informações de identificação serão listadas na seção Recurso dos detalhes de uma descoberta. O tipo de entidade do IAM envolvida pode ser determinado pelo campo Tipo de usuário, o nome da entidade do IAM estará no campo Nome de usuário. O tipo de entidade do IAM envolvida na descoberta também pode ser determinado pelo ID de chave de acesso usado.

Para chaves que começam com `AKIA`:

Esse tipo de chave é uma credencial de longo prazo gerenciada pelo cliente associada a um usuário do IAM ou Usuário raiz da conta da AWS. Para obter informações sobre como gerenciar chaves de acesso para usuários do IAM, consulte Gerenciamento de chaves de acesso de usuários do IAM.

Para chaves que começam com `ASIA`:

Esse tipo de chave é uma credencial temporária de curto prazo gerada pelo AWS Security Token Service. Essas chaves existem por pouco tempo e não podem ser visualizadas ou gerenciadas no AWS Management Console. As funções do IAM sempre usarão AWS STS credenciais, mas também podem ser geradas para usuários do IAM. Para obter mais informações, AWS STS consulte IAM: Credenciais de segurança temporárias.

Se um perfil tiver sido usado, o campo Nome de usuário conterá informações sobre o nome do perfil usado. Você pode determinar como a chave foi solicitada AWS CloudTrail examinando o `sessionIssuer` elemento da entrada do CloudTrail registro. Para obter mais informações, consulte IAM e AWS STS informações em CloudTrail.

2. Revise as permissões para a entidade do IAM.

   Abra o console do IAM. Dependendo do tipo de entidade usada, selecione a guia Usuários ou Funções e localize a entidade afetada digitando o nome identificado no campo de pesquisa. Use as guias Permissão e Consultor de acesso para revisar permissões efetivas para essa entidade.

3. Determine se as credenciais da entidade do IAM foram usadas legitimamente.

   Entre em contato com o usuário das credenciais para determinar se a atividade foi intencional.

   Por exemplo, descubra se o usuário fez o seguinte:

   - Invocou a operação de API listada na descoberta GuardDuty
   - Invocou a operação da API no horário indicado na descoberta do GuardDuty
   - Invocou a operação da API do endereço IP que foi listado na descoberta do GuardDuty

Se essa atividade for um uso legítimo das AWS credenciais, você poderá ignorar a GuardDuty descoberta. O https://console.aws.amazon.com/guardduty/ console permite que você configure regras para suprimir totalmente as descobertas individuais para que elas não apareçam mais. Para obter mais informações, consulte Regras de supressão em GuardDuty.

Se não for possível confirmar se essa atividade é um uso legítimo, isso pode indicar um comprometimento da chave de acesso específica, das credenciais de login do usuário do IAM ou, possivelmente, de toda a Conta da AWS. Se você suspeitar que suas credenciais foram comprometidas, revise as informações em Minha página Conta da AWS pode estar comprometida para corrigir esse problema.

Como corrigir um contêiner autônomo possivelmente comprometido

Quando GuardDuty gera tipos de descoberta que indicam um contêiner potencialmente comprometido, seu tipo de recurso será Contêiner. Caso o comportamento que causou a descoberta seja esperado em seu ambiente, considere usar Regras de supressão.

Para corrigir credenciais potencialmente comprometidas em seu AWS ambiente, execute as seguintes etapas:

1. Isole o contêiner possivelmente comprometido

   As etapas a seguir vão ajudar a identificar o workload do contêiner possivelmente malicioso:

   - Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.
   - Na página Descobertas, escolha a respectiva descoberta para visualizar o painel de descobertas.
   - No painel de descobertas, na seção Recursos afetados, é possível ver o ID e o Nome do contêiner.

   Isole esse contêiner de outras workloads do contêiner.

2. Pause o contêiner

   Suspenda todos os processos no contêiner.

   Para obter informações sobre como congelar seu contêiner, consulte Pausar um contêiner.

   Interrompa o contêiner.

   Se a etapa acima não funcionar e o contêiner não pausar, interrompa a execução do contêiner. Se você tiver ativado o Retenção de snapshots recurso, GuardDuty reterá os instantâneos dos seus volumes do EBS que contêm malware.

Para obter informações sobre como interromper o contêiner, consulte Interromper um contêiner.

3. Avaliar a presença de malware

   Verifique se o malware estava na imagem do contêiner.

A descoberta pode ser ignorada se o acesso foi autorizado. O https://console.aws.amazon.com/guardduty/ console permite que você configure regras para suprimir totalmente as descobertas individuais para que elas não apareçam mais. O GuardDuty console permite que você configure regras para suprimir totalmente as descobertas individuais para que elas não apareçam mais. Para obter mais informações, consulte Regras de supressão em GuardDuty.

Como corrigir as descobertas da Proteção do EKS

GuardDuty A Amazon gera descobertas que indicam possíveis problemas de segurança do Kubernetes quando a Proteção EKS está habilitada para sua conta. Para obter mais informações, consulte Proteção do EKS. As seções a seguir descrevem as etapas de correção recomendadas para qualquer uma das situações. As ações de remediação específicas são descritas na entrada desse tipo específico de descoberta. Para acessar as informações completas sobre um tipo de descoberta selecione-a na tabela Tipos de descobertas ativas.

Se algum dos tipos de descoberta damproteção EKS tiver sido gerado com inesperadamente, considere adicionar Regras de supressão em GuardDuty para evitar futuros alertas.

Diferentes tipos de ataques e problemas de configuração podem desencadear descobertas da Proteção GuardDuty EKS. Este guia ajuda você a identificar as causas principais das GuardDuty descobertas em seu cluster e descreve as diretrizes de remediação apropriadas. A seguir estão as principais causas que levaram às descobertas do GuardDuty Kubernetes:

- Possíveis problemas de configuração
- Como corrigir usuários do Kubernetes possivelmente comprometidos
- Como corrigir pods do Kubernetes possivelmente comprometidos
- Como corrigir pods do Kubernetes potencialmente comprometidos
- Como corrigir imagens de contêiner possivelmente comprometidas

> **Note**
>
> Antes da versão 1.14 do Kubernetes, o `system:unauthenticated` grupo era associado a `system:discovery` e por padrão. `system:basic-user` ClusterRoles Isso pode permitir o acesso não intencional de usuários anônimos. As atualizações de cluster não revogam essas permissões, o que significa que, mesmo que você tenha atualizado seu cluster para a versão 1.14 ou posterior, essas permissões ainda podem estar em vigor. Recomendamos que você desassocie essas permissões do grupo `system:unauthenticated`.
> Para obter mais informações sobre como remover essas permissões, consulte Proteger clusters do Amazon EKS com práticas recomendadas no Guia do usuário do Amazon EKS.

Possíveis problemas de configuração

Se uma descoberta indicar um problema de configuração, consulte a seção de correção dessa descoberta para obter orientação sobre como resolver esse problema específico. Para obter mais informações, consulte os tipos de descoberta a seguir que indicam problemas de configuração:

- Policy:Kubernetes/AnonymousAccessGranted
- Policy:Kubernetes/ExposedDashboard
- Policy:Kubernetes/AdminAccessToDefaultServiceAccount
- Policy:Kubernetes/KubeflowDashboardExposed
- Qualquer descoberta que termine em SuccessfulAnonymousAccess

Como corrigir usuários do Kubernetes possivelmente comprometidos

Uma GuardDuty descoberta pode indicar um usuário comprometido do Kubernetes quando um usuário identificado na descoberta realizou uma ação inesperada da API. Você pode identificar o usuário na seção de detalhes do usuário do Kubernetes de um detalhe da descoberta no console ou no `resource.kubernetesDetails.kubernetesUserDetails` do JSON das descobertas. Esses detalhes do usuário incluem `user name`, `uid` e os grupos do Kubernetes aos quais o usuário pertence.

Se o usuário estava acessando a workload usando uma entidade do IAM, você pode usar a seção `Access Key details` para identificar os detalhes de um usuário ou perfil do IAM. Consulte os seguintes tipos de usuário e suas diretrizes de correção.

> **Note**
>
> Você pode usar o Amazon Detective para investigar melhor o perfil do IAM ou o usuário identificado na descoberta. Ao visualizar os detalhes da descoberta no GuardDuty console, escolha Investigar no Detetive. Em seguida, selecione o AWS usuário ou a função nos itens listados para investigá-la no Detective.

Built-in Kubernetes admin — O usuário padrão atribuído pelo Amazon EKS à identidade do IAM que criou o cluster. Esse tipo de usuário é identificado pelo nome do usuário `kubernetes-admin`.

Para revogar o acesso de um administrador integrado do Kubernetes:

- Identifique o `userType` da seção `Access Key details`.
  - Se o `userType` é Perfil e o perfil pertencer a um perfil de instância do EC2:
    - Identifique essa instância e siga as instruções em Como corrigir uma instância do Amazon EC2 potencialmente comprometida.
  - Se `userType` for Usuário ou for uma Função que foi assumida por um usuário:
    1. Gire a chave de acesso desse usuário.
    2. Alterne todos os segredos aos quais o usuário teve acesso.
    3. Revise as informações em Minha página Conta da AWS que podem estar comprometidas para obter mais detalhes.

Usuário autenticado pelo OIDC: um usuário recebeu acesso por meio de um provedor do OIDC. Normalmente, um usuário do OIDC tem um endereço de e-mail como nome de usuário. Você pode verificar se o cluster usa o OIDC com o seguinte comando: `aws eks list-identity-provider-configs --cluster-name` *`your-cluster-name`*

Para revogar o acesso de um usuário autenticado pelo OIDC:

1. Alterne as credenciais desse usuário no provedor OIDC.
2. Alterne todos os segredos aos quais o usuário teve acesso.

AWS-Usuário ConfigMap definido por autenticação — Um usuário do IAM que recebeu acesso por meio de um AWS-auth. ConfigMap Para obter mais informações, consulte Gerenciar usuários ou perfis do IAM para seu cluster no Guia do usuário do Amazon EKS. É possível revisar as permissões usando este comando: `kubectl edit configmaps aws-auth --namespace kube-system`

Para revogar o acesso de um AWS ConfigMap usuário:

1. Use o comando a seguir para abrir ConfigMap o.

```
kubectl edit configmaps aws-auth --namespace kube-system
```

2. Identifique a função ou a entrada do usuário na seção MapRoles ou MapUsers com o mesmo nome de usuário relatado na seção de detalhes do usuário do Kubernetes de sua descoberta. GuardDuty Veja o exemplo a seguir, em que o usuário administrador foi identificado em uma descoberta.

```
apiVersion: v1
data:
  mapRoles: |
    - rolearn: arn:aws:iam::444455556666:role/eksctl-my-cluster-nodegroup-
standard-wo-NodeInstanceRole-1WP3NUE3O6UCF
      user name: system:node:EC2_PrivateDNSName
      groups:
        - system:bootstrappers
        - system:nodes
  mapUsers: |
    - userarn: arn:aws:iam::123456789012:user/admin
      username: admin
      groups:
        - system:masters
    - userarn: arn:aws:iam::111122223333:user/ops-user
      username: ops-user
      groups:
        - system:masters
```

3. Remova esse usuário do ConfigMap. Veja o exemplo a seguir em que o usuário administrador foi removido.

```
apiVersion: v1
data:
  mapRoles: |
```

```
    - rolearn: arn:aws:iam::111122223333:role/eksctl-my-cluster-nodegroup-
standard-wo-NodeInstanceRole-1WP3NUE3O6UCF
      username: system:node:{{EC2PrivateDNSName}}
      groups:
        - system:bootstrappers
        - system:nodes
  mapUsers: |
    - userarn: arn:aws:iam::111122223333:user/ops-user
      username: ops-user
      groups:
        - system:masters
```

4. Se `userType` for Usuário ou for uma Função que foi assumida por um usuário:
   a. Gire a chave de acesso desse usuário.
   b. Alterne todos os segredos aos quais o usuário teve acesso.
   c. Verifique as informações em Minha AWS conta que podem estar comprometidas para obter mais detalhes.

Se a descoberta não tiver uma seção `resource.accessKeyDetails`, o usuário é uma conta de serviço do Kubernetes.

Conta de serviço: a conta de serviço fornece uma identidade para pods e pode ser identificada por um nome de usuário com o seguinte formato: `system:serviceaccount:`*`namespace`*`:`*`service_account_name`*.

Para revogar o acesso a uma conta de serviço:

1. Alterne as credenciais da conta de serviço.
2. Revise a orientação sobre comprometimento de pods na seção a seguir.

Como corrigir pods do Kubernetes possivelmente comprometidos

Quando GuardDuty especifica detalhes de um pod ou recurso de carga de trabalho dentro da `resource.kubernetesDetails.kubernetesWorkloadDetails` seção, esse recurso de pod ou carga de trabalho foi potencialmente comprometido. Uma GuardDuty descoberta pode indicar que um único pod foi comprometido ou que vários pods foram comprometidos por meio de um recurso de nível superior. Consulte os seguintes cenários de comprometimento para obter orientação sobre como identificar o pod ou os pods que foram comprometidos.

Comprometimento de pods individuais

Se o campo `type` dentro da seção `resource.kubernetesDetails.kubernetesWorkloadDetails` for pods, a descoberta identifica um único pod. O campo de nome é o `name` dos pods e o campo `namespace` é seu namespace.

Para informações sobre como identificar o nó de processamento que executa os pods, consulte Identificar o nó de processamento e pods ofensivos no Guia de práticas recomendadas do Amazon EKS.

Pods comprometidos por meio de recursos de workload

Se o campo `type` dentro da seção `resource.kubernetesDetails.kubernetesWorkloadDetails` identificar um Recurso de workload, como um `Deployment`, é provável que todos os pods desse recurso de workload tenham sido comprometidos.

Para obter informações sobre como identificar todos os pods do recurso de workload e os nós nos quais estão sendo executados, consulte Identificar os nós de processamento e pods ofensivos usando o nome de workload no Guia de práticas recomendadas do Amazon EKS.

Pods comprometidos por meio da conta de serviço

Se uma GuardDuty descoberta identificar uma conta de serviço na `resource.kubernetesDetails.kubernetesUserDetails` seção, é provável que os pods que usam a conta de serviço identificada estejam comprometidos. O nome de usuário relatado por uma descoberta é uma conta de serviço se tiver o seguinte formato: `system:serviceaccount:`*`namespace`*`:`*`service_account_name`*.

Para obter informações sobre como identificar todos os pods usando a conta de serviço e os nós nos quais estão sendo executados, consulte Identificar os nós de processamento e pods ofensivos usando o nome da conta de serviço no Guia de práticas recomendadas do Amazon EKS.

Depois de identificar todos os pods comprometidos e os nós em que eles estão sendo executados, consulte Isolar o pod criando uma política de rede que negue todo o tráfego de entrada e saída do pod no Guia de práticas recomendadas do Amazon EKS.

Para corrigir um pod possivelmente comprometido:

1. Identifique a vulnerabilidade que comprometeu os pods.
2. Implemente a correção para essa vulnerabilidade e inicie novos pods de substituição.
3. Exclua os pods vulneráveis.

   Para obter mais informações, consulte Reimplantar o recurso de workload ou o pod comprometido no Guia de práticas recomendadas do Amazon EKS.

Se o node de trabalho tiver recebido uma função do IAM que permite que os pods tenham acesso a outros AWS recursos, remova essas funções da instância para evitar maiores danos causados pelo ataque. Da mesma forma, se o pod tiver recebido uma função do IAM, avalie se você pode remover com segurança as políticas do IAM da função sem afetar outras workloads.

Como corrigir imagens de contêiner possivelmente comprometidas

Quando uma GuardDuty descoberta indica o comprometimento de um pod, a imagem usada para iniciar o pod pode ser potencialmente maliciosa ou estar comprometida. GuardDuty as descobertas identificam a imagem do contêiner dentro do `resource.kubernetesDetails.kubernetesWorkloadDetails.containers.image` campo. Você pode determinar se a imagem é mal-intencionada examinando-a em busca de malware.

Para corrigir uma imagem de contêiner potencialmente comprometida:

1. Pare de usar a imagem imediatamente e remova-a do seu repositório de imagens.
2. Identifique todos os pods usando a imagem possivelmente comprometida.

   Para obter mais informações, consulte Identificar nós de processamento e pods com imagens comprometidas ou vulneráveis no Guia de práticas recomendadas do Amazon EKS.
3. Isole os pods potencialmente comprometidos, alterne as credenciais e colete dados para análise. Para obter mais informações, consulte Isolar o pod criando uma política de rede que negue todo o tráfego de entrada e saída para o pod no Guia de práticas recomendadas do Amazon EKS.
4. Identifique todos os pods usando a imagem potencialmente comprometida.

Como corrigir pods do Kubernetes potencialmente comprometidos

Uma GuardDuty descoberta pode indicar um comprometimento do nó se o usuário identificado na descoberta representar a identidade do nó ou se a descoberta indicar o uso de um contêiner privilegiado.

A identidade do usuário é um nó de processamento se o campo nome de usuário tiver o seguinte formato: `system:node:node name`. Por exemplo, .`system:node:ip-192-168-3-201.ec2.internal` Isso indica que o adversário obteve acesso ao nó e está usando as credenciais do nó para se comunicar com o endpoint da API do Kubernetes.

Uma descoberta indica o uso de um contêiner privilegiado se um ou mais dos contêineres listados na descoberta tiver o campo de descoberta `resource.kubernetesDetails.kubernetesWorkloadDetails.containers.securityContext.` definido como `True`.

Para corrigir um nó possivelmente comprometido:

1. Isole o pod comprometido, alterne as credenciais e colete dados para análise.

   Para obter mais informações, consulte Isolar o pod criando uma política de rede que negue todo o tráfego de entrada e saída para o pod no Guia de práticas recomendadas do Amazon EKS.
2. Identifique as contas de serviço usadas por todos os pods em execução no nó potencialmente comprometido. Revise suas permissões e alterne as contas de serviço, se necessário.
3. Encerre o nó possivelmente comprometido.

Como corrigir as descobertas do Monitoramento de runtime

Quando você ativa o Runtime Monitoring para sua conta, a Amazon GuardDuty pode gerar GuardDuty Tipos de descoberta de monitoramento de tempo de execução dados que indiquem possíveis problemas de segurança em seu AWS ambiente. Os possíveis problemas de segurança indicam uma instância do Amazon EC2 comprometida, uma carga de trabalho do contêiner, um cluster do Amazon EKS ou um conjunto de credenciais comprometidas em seu ambiente. AWS O atendente de segurança monitora eventos de runtime para vários tipos de recursos. Para identificar o recurso potencialmente comprometido, visualize o tipo de recurso nos detalhes de descoberta gerados no GuardDuty console. A seção a seguir descreve as etapas de correção recomendadas para qualquer tipo de recurso.

Instance

Se o Tipo de recurso nos detalhes da descoberta for Instância, isso indica que uma instância do EC2 ou um nó do EKS está potencialmente comprometida.

- Para corrigir um nó EKS comprometido, consulte Como corrigir pods do Kubernetes potencialmente comprometidos.
- Para corrigir uma instância do EC2 comprometida, consulte Como corrigir uma instância do Amazon EC2 potencialmente comprometida.

EKSCluster

Se o Tipo de recurso nos detalhes da descoberta for EKSCluster, isso indica que um pod ou um contêiner dentro de um cluster do EKS está potencialmente comprometido.

- Para corrigir um pod comprometido, consulte Como corrigir pods do Kubernetes possivelmente comprometidos.
- Para corrigir uma imagem de contêiner comprometida, consulte Como corrigir imagens de contêiner possivelmente comprometidas.

ECSCluster

Se o Tipo de recurso nos detalhes da descoberta for EKSCluster, isso indica que uma tarefa ECS ou um contêiner dentro de um cluster de tarefa EKS está potencialmente comprometido.

1. Identifique o cluster do ECS afetado.

   A descoberta do GuardDuty Runtime Monitoring fornece os detalhes do cluster ECS no painel de detalhes da descoberta ou na `resource.ecsClusterDetails` seção do JSON de descoberta.

2. Identificar a tarefa do ECS afetada

   A descoberta do GuardDuty Runtime Monitoring fornece os detalhes da tarefa do ECS no painel de detalhes da descoberta ou na `resource.ecsClusterDetails.taskDetails` seção do JSON de descoberta.

3. Isolar a tarefa afetada

Isole a tarefa afetada negando todo o tráfego de entrada e saída dessa tarefa. Uma regra para negar todo o tráfego pode ajudar a interromper um ataque em andamento, cortando todas as conexões com a tarefa.

4. Corrigir a tarefa comprometida
   a. Identifique a vulnerabilidade que comprometeu a tarefa.
   b. Implemente a correção para essa vulnerabilidade e inicie uma nova tarefa de substituição.
   c. Parar a tarefa vulnerável.

Container

Se o Tipo de recurso nos detalhes da descoberta for Contêiner, isso indica que um contêiner autônomo está potencialmente comprometido.

- Para corrigir, consulte Como corrigir um contêiner autônomo possivelmente comprometido.
- Se a descoberta for gerada em vários contêineres usando a mesma imagem de contêiner, consulte Como corrigir imagens de contêiner possivelmente comprometidas.
- Se o contêiner acessou o host EC2 subjacente, suas credenciais de instância associadas podem ter sido comprometidas. Para obter mais informações, consulte Correção de problemas potencialmente comprometidos AWS credenciais.
- Se um agente potencialmente mal-intencionado acessou o nó EKS subjacente ou uma instância do EC2, consulte a correção recomendada nas guias EKSCluster e Instance.

Como corrigir imagens de contêiner comprometidas

Quando uma GuardDuty descoberta indica um comprometimento da tarefa, a imagem usada para iniciar a tarefa pode ser maliciosa ou estar comprometida. GuardDuty as descobertas identificam a imagem do contêiner dentro do `resource.ecsClusterDetails.taskDetails.containers.image` campo. Você pode determinar se a imagem é mal-intencionada examinando-a em busca de malware.

Para corrigir uma imagem de contêiner comprometida

1. Pare de usar a imagem imediatamente e remova-a do seu repositório de imagens.
2. Identificar todas as tarefas que estão usando essa imagem.

3. Interromper todas as tarefas que estão usando a imagem comprometida. Atualizar suas configurações de tarefas para que parem de usar a imagem comprometida.

Corrigir um banco de dados possivelmente comprometido

GuardDuty gerados Tipos de descoberta da Proteção do RDS que indicam um comportamento de login potencialmente suspeito e anômalo Bancos de dados compatíveis após a ativação. Proteção do RDS Usando a atividade de login do RDS, GuardDuty analisa e traça perfis de ameaças identificando padrões incomuns nas tentativas de login.

> **Note**
>
> Você pode acessar as informações completas sobre um tipo de descoberta selecionando-o na GuardDuty tipos de descoberta ativa.

Siga estas etapas recomendadas para corrigir um banco de dados Amazon Aurora potencialmente comprometido em seu ambiente. AWS

Tópicos

- Corrigir um banco de dados potencialmente comprometido com eventos de login bem-sucedidos
- Corrigindo um banco de dados potencialmente comprometido com eventos de login falhados
- Corrigindo um banco de dados potencialmente comprometido com atividade de exfiltração anômala
- Corrigindo um banco de dados potencialmente comprometido com atividade destrutiva anômala
- Corrigir remediar credenciais potencialmente comprometidas
- Restringir o acesso à rede

Corrigir um banco de dados potencialmente comprometido com eventos de login bem-sucedidos

As etapas recomendadas a seguir podem ajudar você a corrigir um banco de dados Aurora potencialmente comprometido que apresenta um comportamento incomum relacionado a eventos de login bem-sucedidos.

1. Identifique o banco de dados e o usuário afetados.

   A GuardDuty descoberta gerada fornece o nome do banco de dados afetado e os detalhes do usuário correspondentes. Para obter mais informações, consulte Detalhes da descoberta.

2. Confirme se esse comportamento é esperado ou inesperado.

   A lista a seguir especifica possíveis cenários que podem ter causado GuardDuty a geração de uma descoberta:

   - Um usuário que faz login em seu banco de dados após um longo período de tempo.
   - Um usuário que faz login em seu banco de dados ocasionalmente, por exemplo, um analista financeiro que faz login a cada trimestre.
   - Um agente potencialmente suspeito envolvido em uma tentativa bem-sucedida de login pode comprometer o banco de dados.

3. Comece esta etapa se o comportamento for inesperado.

   1. Restringir acesso ao banco

      Restrinja o acesso ao banco de dados para as contas suspeitas e a origem dessa atividade de login. Para obter mais informações, consulte Corrigir remediar credenciais potencialmente comprometidas e Restringir o acesso à rede.

   2. Avalie o impacto e determine quais informações foram acessadas.

      - Se disponíveis, revise os registros de auditoria para identificar as informações que podem ter sido acessadas. Para obter mais informações, consulte Monitorar eventos, logs e streams em um cluster de banco de dados do Amazon Aurora no Guia do usuário do Amazon Aurora.
      - Determine se alguma informação confidencial ou protegida foi acessada ou modificada.

Corrigindo um banco de dados potencialmente comprometido com eventos de login falhados

As etapas recomendadas a seguir podem ajudar você a corrigir um banco de dados Aurora potencialmente comprometido que apresenta um comportamento incomum relacionado a eventos de login com falha.

1. Identifique o banco de dados e o usuário afetados.

A GuardDuty descoberta gerada fornece o nome do banco de dados afetado e os detalhes do usuário correspondentes. Para obter mais informações, consulte Detalhes da descoberta.

2. Identifique a origem das tentativas de login malsucedidas.

   A GuardDuty descoberta gerada fornece o endereço IP e a organização ASN (se for uma conexão pública) na seção Ator do painel de descoberta.

   Um Autonomous System (AS – Sistema autônomo) é um grupo de um ou mais prefixos de IP (listas de endereços de IP acessíveis em uma rede) executados por uma ou mais operadoras de rede que mantêm uma política de roteamento única e claramente definida. As operadoras de rede precisam de Autonomous System Numbers (ASNs – Números de sistema autônomo) para controlar o roteamento em suas redes e trocar informações de roteamento com outros provedores de serviços de Internet (ISPs).

3. Confirme se esse comportamento é inesperado.

   Examine se essa atividade representa uma tentativa de obter acesso não autorizado adicional ao banco de dados da seguinte forma:

   - Se a fonte for interna, verifique se uma aplicação está configurado incorretamente e está tentando se conectar repetidamente.
   - Se for um ator externo, examine se o banco de dados correspondente está voltado para o público ou está mal configurado, permitindo que possíveis agentes mal-intencionados usem nomes de usuários comuns com força bruta.

4. Comece esta etapa se o comportamento for inesperado.

   1. Restringir acesso ao banco

      Restrinja o acesso ao banco de dados para as contas suspeitas e a origem dessa atividade de login. Para obter mais informações, consulte Corrigir remediar credenciais potencialmente comprometidas e Restringir o acesso à rede.

   2. Faça uma análise da causa raiz e determine as etapas que potencialmente levaram a essa atividade.

      Configure um alerta para ser notificado quando uma atividade modifica uma política de rede e cria um estado inseguro. Para obter mais informações, consulte Políticas de firewall no AWS Network Firewall no Guia do desenvolvedor do AWS Network Firewall .

Corrigindo um banco de dados potencialmente comprometido com atividade de exfiltração anômala

As etapas recomendadas a seguir podem ajudá-lo a corrigir um banco de dados Aurora potencialmente comprometido que apresenta um comportamento incomum relacionado a eventos de exfiltração de dados.

1. Identifique o banco de dados e o usuário afetados.

   A GuardDuty descoberta gerada fornece o nome do banco de dados afetado e os detalhes do usuário correspondentes. Para obter mais informações, consulte Detalhes da descoberta.

2. Identifique o escopo dos dados acessados.

   Analise os registros de atividades de dados do RDS disponíveis para determinar quais tabelas e linhas foram acessadas pelo usuário anômalo durante a janela de tempo indicada pela descoberta. Avalie a sensibilidade dos dados que foram potencialmente exfiltrados.

3. Confirme se esse comportamento é inesperado.

   Examine se essa atividade representa um comportamento operacional legítimo da seguinte forma:

   - Se a origem for interna, examine se uma tarefa de ETL agendada, uma ferramenta de geração de relatórios ou um processo de backup podem explicar o volume elevado de consultas.
   - Se for um ator externo ou um atributo de banco de dados nunca antes visto, examine se as credenciais do banco de dados correspondentes podem ter sido expostas ou compartilhadas externamente.
   - Verifique se a combinação de volume e atributos não vistos (endereço IP, ASN, nome do aplicativo) está alinhada com alguma alteração operacional conhecida.

4. Comece esta etapa se o comportamento for inesperado.

   Revogue o acesso e alterne as credenciais.

   Altere imediatamente a senha do usuário do banco de dados afetado e revogue as sessões ativas. Se o usuário tiver privilégios elevados, restrinja temporariamente suas permissões para somente leitura ou remova totalmente o acesso até que a investigação seja concluída.

5. Avalie o impacto nos negócios.

Identifique os dados que estavam acessíveis ao usuário afetado, determine se algum dado confidencial ou regulamentado (PII, financeiro, de saúde) foi potencialmente exfiltrado e siga os procedimentos de notificação de violação de dados da sua organização, se aplicável.

6. Restrinja o acesso à rede.

   Restrinja o acesso ao banco de dados para as contas suspeitas e a origem dessa atividade. Coloque o banco de dados em uma VPC privada, se ainda não estiver configurado, e limite as regras do grupo de segurança para permitir tráfego somente das fontes necessárias. Para obter mais informações, consulte Restringir o acesso à rede.

7. Faça uma análise da causa raiz e determine as etapas que potencialmente levaram a essa atividade.

   Configure um alerta para ser notificado quando uma atividade modifica uma política de rede e cria um estado inseguro. Para obter mais informações, consulte Políticas de firewall no AWS Network Firewall no Guia do desenvolvedor do AWS Network Firewall .

Corrigindo um banco de dados potencialmente comprometido com atividade destrutiva anômala

As etapas recomendadas a seguir podem ajudá-lo a corrigir um banco de dados Aurora potencialmente comprometido que apresenta um comportamento incomum relacionado a eventos ou destrutivos. `DELETE` `DROP`

1. Identifique o banco de dados e o usuário afetados.

   A GuardDuty descoberta gerada fornece o nome do banco de dados afetado e os detalhes do usuário correspondentes. Para obter mais informações, consulte Detalhes da descoberta.

2. Identifique o escopo das operações destrutivas.

   Analise os registros de atividades de dados do RDS disponíveis para determinar quais tabelas, linhas ou objetos de banco de dados foram excluídos ou descartados pelo usuário anômalo durante a janela de tempo indicada pela descoberta. Determine se a perda de dados pode ser recuperada de backups ou instantâneos existentes.

3. Confirme se esse comportamento é inesperado.

   Examine se essa atividade representa um comportamento operacional legítimo da seguinte forma:

- Se a origem for interna, examine se um trabalho de manutenção programado, um script de limpeza ou um processo de migração podem explicar as `DROP` operações `DELETE` ou.
- Se for um ator externo ou um atributo de banco de dados nunca antes visto, examine se as credenciais do banco de dados correspondentes podem ter sido expostas ou comprometidas.
- Verifique se a combinação de operações destrutivas e atributos invisíveis (endereço IP, ASN, nome do aplicativo) está alinhada com alguma alteração operacional conhecida.

4. Comece esta etapa se o comportamento for inesperado.

   Revogue o acesso e alterne as credenciais.

   Altere imediatamente a senha do usuário do banco de dados afetado e revogue as sessões ativas. Remova os `DELETE` privilégios `DROP` e privilégios do usuário até que a investigação seja concluída para evitar mais destruição de dados.

5. Inicie a recuperação de dados.

   Se a perda de dados for confirmada, inicie a recuperação pontual a partir de backups automatizados ou restaure a partir do snapshot mais recente. Para o Amazon Aurora, você pode usar o backtrack para retroceder o banco de dados até um momento anterior à ocorrência da atividade destrutiva. Para o Amazon RDS, use a recuperação pontual para restaurar até um ponto antes do evento.

6. Restrinja o acesso à rede e fortaleça as permissões.

   Restrinja o acesso ao banco de dados para as contas suspeitas e a origem dessa atividade. Coloque o banco de dados em uma VPC privada, se ainda não estiver configurado, e limite as regras do grupo de segurança para permitir tráfego somente das fontes necessárias. Analise as políticas do IAM e os privilégios de usuário do banco de dados para impor o acesso com privilégios mínimos e habilite a proteção contra exclusão na instância do RDS, caso ainda não esteja habilitada. Para obter mais informações, consulte Restringir o acesso à rede.

7. Faça uma análise da causa raiz e determine as etapas que potencialmente levaram a essa atividade.

   Configure um alerta para ser notificado quando uma atividade modifica uma política de rede e cria um estado inseguro. Para obter mais informações, consulte Políticas de firewall no AWS Network Firewall no Guia do desenvolvedor do AWS Network Firewall .

Corrigir remediar credenciais potencialmente comprometidas

Uma GuardDuty descoberta pode indicar que as credenciais do usuário de um banco de dados afetado foram comprometidas quando o usuário identificado na descoberta executou uma operação inesperada no banco de dados. Você pode identificar o usuário na seção de detalhes do usuário do RDS DB no painel de descoberta no console ou no `resource.rdsDbUserDetails` do JSON das descobertas. Esses detalhes do usuário incluem nome de usuário, aplicativo usado, banco de dados acessado, versão SSL e método de autenticação.

- Para revogar o acesso ou alternar senhas de usuários específicos envolvidos na descoberta, consulte Segurança com o Amazon Aurora MySQL ou Segurança com o Amazon Aurora PostgreSQL no Guia do usuário do Amazon Aurora.
- Use AWS Secrets Manager para armazenar com segurança e alternar automaticamente os segredos dos bancos de dados do Amazon Relational Database Service (RDS). Para obter mais informações, consulte Tutoriais do AWS Secrets Manager, no Guia do usuário do AWS Secrets Manager .
- Use a autenticação do banco de dados do IAM para gerenciar o acesso dos usuários do banco de dados sem a necessidade de senhas. Para obter mais informações, consulte Autenticação de banco de dados do IAM no Guia do usuário do Amazon Aurora.

  Para obter mais informações, consulte Práticas recomendadas de segurança do Amazon Relational Database Service no Guia do usuário do Amazon RDS.

Restringir o acesso à rede

Uma GuardDuty descoberta pode indicar que um banco de dados está acessível além de seus aplicativos ou da Virtual Private Cloud (VPC). Se o endereço IP remoto na descoberta for uma fonte de conexão inesperada, audite os grupos de segurança. Uma lista de grupos de segurança anexados ao banco de dados está disponível em Grupos de segurança no https://console.aws.amazon.com/rds/console ou no JSON `resource.rdsDbInstanceDetails.dbSecurityGroups` das descobertas. Para obter mais informações sobre a configuração de grupos de segurança, consulte Controlar acesso com grupos de segurança no Guia do usuário do Amazon RDS.

Se você estiver usando um firewall, restrinja o acesso à rede ao banco de dados reconfigurando as Network Access Control Lists (NACLs – Listas de controle de acesso à rede). Para obter mais

informações, consulte Firewalls no AWS Network Firewall no Guia do desenvolvedor do AWS Network Firewall .

Correção de uma função do Lambda comprometida

Quando GuardDuty geradaTipos de descoberta da Proteção do Lambda, sua função Lambda pode ser comprometida. Se a atividade que causou GuardDuty a geração dessa descoberta era esperada, você pode considerar usarRegras de supressão. Recomendamos concluir as etapas a seguir para corrigir uma função do Lambda comprometida.

Para corrigir as descobertas da Proteção do Lambda

1. Identifique a versão da função Lambda potencialmente comprometida.

   Uma GuardDuty descoberta para o Lambda Protection fornece o nome, o Amazon Resource Name (ARN), a versão da função e o ID da revisão associados à função Lambda listada nos detalhes da descoberta.
2. Identifique a origem da atividade suspeita.

   a. Analise o código associado à versão da função do Lambda envolvida na descoberta.
   b. Analise as bibliotecas e camadas importadas da versão da função do Lambda envolvida na descoberta.
   c. Se você ativou AWS Lambda as funções de digitalização com o Amazon Inspector, revise as descobertas do Amazon Inspector associadas à função Lambda envolvida na descoberta.
   d. Analise os AWS CloudTrail registros para identificar o principal que causou a atualização da função e garantir que a atividade foi autorizada ou esperada.
3. Corrija a função do Lambda potencialmente comprometida.

   a. Desabilite os acionadores de execução da função do Lambda envolvida na descoberta. Para obter mais informações, consulte DeleteFunctionEventInvokeConfig.
   b. Revise o código do Lambda e atualize as importações de bibliotecas e as camadas da função do Lambda para remover as bibliotecas e camadas potencialmente suspeitas.
   c. Mitigue as descobertas do Amazon Inspector relacionadas à função do Lambda envolvida na descoberta.

Monitorando GuardDuty o uso e estimando custos

GuardDuty fornece métricas de uso que rastreiam o processamento de planos de proteção, fontes de dados logs/events e vCPUs monitoradas em GuardDuty tempo de execução ao longo do tempo.

Nesta página:

- Métricas CloudWatch de uso da Amazon
- Entendendo GuardDuty o uso
- Estimando GuardDuty o custo

Métricas CloudWatch de uso da Amazon

GuardDuty publica métricas de uso na Amazon CloudWatch, permitindo que você:

- Acompanhe o uso real ao longo do tempo
- Crie painéis e alarmes personalizados
- Exporte dados de uso para estimativa de custos na Calculadora AWS de Preços

GuardDuty as métricas de uso são publicadas com base na configuração da sua conta:

- Todas as contas (autônomas, de administrador delegado e contas de membros) recebem métricas de uso de contas individuais na Amazon CloudWatch
- Além disso, as contas de administrador delegadas recebem métricas de uso agregadas para toda a organização.

GuardDuty as métricas de uso são publicadas na Amazon em CloudWatch 24 horas.

Detalhes métricos

GuardDuty publica as seguintes métricas `Hourly` de uso na Amazon CloudWatch sob o `AWS/GuardDuty` namespace:

Plano de proteção	Fonte de dados	Nome da métrica	Unidade	Descrição

Detecção básica de ameaças	CloudTrailEvents	AnalyzedCount	Contagem	Número de eventos CloudTrail de gerenciamento analisados
Detecção básica de ameaças	VPCFlowLogDNSLogEvents	AnalyzedBytes	Bytes	Volume de registros de fluxo de VPC e registros de DNS analisados
Proteção do EKS	KubernetesAuditLogs	AnalyzedCount	Contagem	Número de eventos de log de auditoria do Amazon EKS analisados
Proteção do S3	S3DataEvents	AnalyzedCount	Contagem	Número de eventos de dados do S3 analisados
Monitoramento de runtime	RuntimeMonitoringEC2	MonitoredVcpuHours	Contagem (vCPU-Hours)	Horas de vCPU do EC2 monitoradas pelo Runtime Monitoring
Monitoramento de runtime	RuntimeMonitoringEKS	MonitoredVcpuHours	Contagem (vCPU-Hours)	Horas de vCPU do Amazon EKS monitoradas pelo Runtime Monitoring

Monitoramento de runtime	RuntimeMonitoringFargate	MonitoredVcpuHours	Contagem (vCPU-Hours)	Horas de vCPU do Fargate monitoradas pelo Runtime Monitoring
Proteção contra malware para o EC2	OnDemandEBSSnapshot	ScannedBytes	Bytes	Volume de dados de snapshot do EBS sob demanda digitalizados
Proteção contra malware para o EC2	OnDemandEBSVolume	ScannedBytes	Bytes	Volume de dados de volume do EBS sob demanda digitalizados
Proteção contra malware para o EC2	MalwareProtectionEBS	ScannedBytes	Bytes	Volume de dados do EBS escaneados pelo Malware Protection
Proteção do RDS	RDS	MonitoredAcuHours	Contagem (ACU-Hours)	Unidades de capacidade do Amazon RDS Aurora monitoradas
Proteção do RDS	RDS ilimitado	MonitoredAcuHours	Contagem (ACU-Hours)	Amazon RDS Aurora Limitless : horas de ACU monitoradas

Proteção do RDS	AuroraScaleout	Monitored AcuHours	Contagem (ACU-Hours)	Horas de ACU do Aurora Scaleout monitoradas
Proteção do RDS	RDS	Monitored VcpuHours	Contagem (vCPU-Hours)	Horas de vCPU do Amazon RDS monitoradas
Proteção do Lambda	LambdaNetworkLogs	AnalyzedBytes	Bytes	Volume de registros de rede Lambda analisados
Proteção de IA	AIDataEvents	AnalyzedBytes	Bytes	Volume de eventos de dados de IA analisados

Dimensões das métricas

- Todas as contas (autônomas, de administrador delegado e contas de membros): as métricas incluem as dimensões `AccountId` e. `DataSource`
- Contas de administrador delegadas: as métricas também incluem `DataSource` dimensões agregadas em todas as contas membros da organização.

Proteção contra malware para S3

GuardDuty `Malware Protection for S3`O plano de proteção publica as seguintes métricas de uso na Amazon CloudWatch sob o `AWS/GuardDuty/MalwareProtection` namespace:

Nome da métrica	Unidade	Descrição
CompletedScanCount	Contagem	O número de verificações de malware de objetos do S3

		concluídos em um determina do período de tempo.
FailedScanCount	Contagem	O número de verificações de malware de objetos do S3 que falharam em um determinado período de tempo.
SkippedScanCount	Contagem	O número de verificações de malware de objetos do S3 que foram ignorados em um determinado período de tempo.
InfectedScanCount	Contagem	O número de verificações de malware de objetos do S3 que detectaram objetos potencialmente maliciosos em um determinado período de tempo.
CompletedScanBytes	Contagem	O número de bytes de objetos do S3 verificados em um determinado período de tempo.

Dimensões das métricas

- Todas as métricas incluem `Malware Protection Plan Id, Resource Name` dimensões
- SkippedScanCount métrica inclui `Skipped Reason` como uma dimensão adicional

Entendendo GuardDuty o uso

GuardDuty Processamento de eventos

Quando ativado, consome GuardDuty automaticamente eventos e registros diretamente das fontes de registro selecionadas Região da AWS. GuardDuty ingere eventos de fontes de dados separadas e independentes para fornecer um valor de segurança abrangente.

> **Important**
>
> Suas regras individuais de configuração ou filtragem de registros de serviços (para registros de fluxo de VPC, registros de DNS, CloudTrail eventos, eventos de dados do S3, registros de auditoria do Kubernetes e registros de rede Lambda) não afetam o processado por. logs/events GuardDuty

GuardDuty Cobranças de processamento do VPC Flow Logs para instâncias monitoradas pelo GuardDuty Runtime Monitoring

Para instâncias monitoradas pelo GuardDuty Runtime Monitoring (por meio do agente EC2 Runtime ou do Amazon EKS Runtime agent), não GuardDuty cobraremos pelo processamento de registros de fluxo do VPC, desde que o agente envie ativamente dados de eventos de tempo de execução. Se o agente parar de transmitir os dados do evento, GuardDuty voltará à cobrança por meio dos registros de fluxo da VPC.

A ativação do monitoramento de tempo de execução diminui o uso de registros de fluxo de VPC nas métricas de CloudWatch uso GuardDuty da Amazon. A desativação do monitoramento de tempo de execução restaura o uso dos registros de fluxo da VPC.

Estimando GuardDuty o custo

GuardDuty oferece um teste gratuito de 30 dias por AWS conta para a maioria dos planos de proteção. Durante esse período de teste, você pode:

- Monitore seu uso real por meio de métricas GuardDuty de uso
- Estime seus custos mensais usando a Calculadora de AWS Preços com base nos padrões de uso observados

Os seguintes planos de proteção incluem um teste gratuito de 30 dias:

- Detecção básica de ameaças
- Proteção do S3
- Proteção do EKS
- Monitoramento de runtime
- Proteção do RDS
- Proteção do Lambda
- Proteção de IA
- Proteção contra malware para EC2 (somente para GuardDuty-initiated escaneamentos quando habilitada com o Foundational Threat Detection)

Utilizar AWS Calculadora de preços

Você pode usar a Calculadora de AWS preços para estimar seus GuardDuty custos mensais com base nos padrões de uso observados. Para criar uma estimativa para GuardDuty:

1. Abra a calculadora AWS de preços.
2. Selecione Criar estimativa.
3. Na página Adicionar serviço, pesquise Amazon GuardDuty e escolha Configurar.
4. Selecione Região da AWS onde GuardDuty está ativado.
5. Na seção Configurações do serviço, insira seu uso estimado para cada plano de proteção com base nas métricas de uso observadas na Amazon CloudWatch ou no GuardDuty console.
6. Escolha Adicionar à minha estimativa para ver o custo mensal projetado.

> **Note**
>
> Algumas métricas GuardDuty de uso são relatadas em bytes. Ao inserir valores na Calculadora de AWS preços, talvez seja necessário converter bytes na unidade apropriada (MB, GB ou TB). Use as seguintes conversões:
>
> - 1 MB = 1.048.576 bytes
> - 1 GB = 1.073.741.824 bytes

- 1 TB = 1.099.511.627.776 bytes

Clientes do Security Hub

O Security Hub oferece um modelo de preços simplificado para detecção de GuardDuty ameaças com seu plano complementar de análise de ameaças, consolidando a medição de várias. GuardDuty DataSources Ao usar o plano de análise de ameaças do Security Hub (Security Hub com GuardDuty):

- Vários GuardDuty DataSources são consolidados
- Notavelmente, para simplificar, os eventos do Amazon EKS Audit Logs e os eventos do S3 Data são convertidos em GB usando uma taxa de conversão fixa.

Para criar uma estimativa de custo do Security Hub, consulte a Documentação do AWS Security Hub.

Observação: GuardDuty o status de teste gratuito de 30 dias é independente da integração com o Security Hub. Ativando ou desativando o Security Hub:

- Não concede um novo teste gratuito se você já tiver usado GuardDuty o período de teste
- Não interrompe nem reinicia um teste gratuito em andamento
- Não estende os períodos de teste existentes

Nomes de recursos para planos de proteção na GuardDuty API

Quando você ativa a Amazon GuardDuty pela primeira vez, ela começa a ser processada Fontes de dados fundamentais em seu AWS ambiente. GuardDuty usa essas fontes de dados para processar um fluxo independente de eventos, como registros de fluxo de VPC, registros de DNS e AWS CloudTrail eventos de gerenciamento. Em seguida, ele analisa esses eventos para identificar possíveis ameaças à segurança e gera descobertas em sua conta.

Quando um ou mais planos de proteção estão habilitados, GuardDuty usa dados adicionais de outros AWS serviços em seu AWS ambiente para monitorar e analisar possíveis ameaças à segurança. Essas fontes de dados adicionais são chamadas de atributos.

Mudar de fontes de dados para atributos

Ao adicionar GuardDuty proteções adicionais, como S3 Protection, Runtime Monitoring, Lambda Protection e outras, você pode configurar o GuardDuty recurso correspondente ao plano de proteção. Historicamente, GuardDuty as proteções eram chamadas `dataSources` nas APIs. No entanto, após março de 2023, os novos planos de GuardDuty proteção agora estão `features` configurados como ou não`dataSources`. GuardDuty ainda oferece suporte à configuração de planos de proteção lançados antes de março de 2023, como `dataSources` por meio da API, mas os novos planos de proteção só estão disponíveis como`features`. Para obter informações sobre quais planos de proteção foram afetados, consulte GuardDuty Mudanças na API.

Se você gerencia planos de GuardDuty configuração e proteção por meio do console, não será diretamente afetado por essa alteração e não precisará realizar nenhuma ação. Essa alteração afeta o comportamento das APIs que são invocadas para habilitar GuardDuty ou proteger planos internos. GuardDuty Se você usa APIs ou AWS CLI para habilitar ou editar a configuração de um plano de proteção, deverá usar o nome do recurso associado. Para obter mais informações, consulte Como mapear `dataSources` para `features`.

GuardDuty Mudanças na API em março de 2023

As GuardDuty APIs configuram recursos de proteção que não pertencem à lista deGuardDuty fontes de dados fundamentais. Um objeto de atributo contém detalhes do recurso, como nome e status do

atributo, e pode conter configurações adicionais para alguns planos de proteção. Essa migração afeta as seguintes APIs na Amazon GuardDuty API Reference:

- CreateDetector
- GetDetector
- UpdateDetector
- GetMemberDetectors
- UpdateMemberDetectors
- DescribeOrganizationConfiguration
- UpdateOrganizationConfiguration
- GetRemainingFreeTrialDays
- GetUsageStatistics

Comparação de atributos com fontes de dados

Historicamente, todos os GuardDuty recursos eram passados por meio de um `dataSources` objeto na API. A partir de março de 2023, GuardDuty prefere o `features` objeto em vez do `dataSources` objeto na API. Todas as fontes de dados anteriores têm seus respectivos atributos, mas os mais recentes podem não ter suas respectivas fontes de dados.

A lista a seguir mostra a comparação entre os objetos `dataSources` e `features` ao passarem por uma API:

- O objeto `dataSources` contém objetos para cada tipo de proteção e seu status. O `features` objeto é uma lista de recursos disponíveis que correspondem a cada tipo de proteção contido nele GuardDuty.

  A partir de março de 2023, a ativação de recursos será a única forma de configurar novos GuardDuty recursos em seu AWS ambiente.
- O `dataSources` esquema na solicitação ou resposta da API é o mesmo em todos os Região da AWS lugares GuardDuty disponíveis. No entanto, é possível que nem todos os atributos estejam disponíveis em cada região. Portanto, os nomes dos atributos disponíveis podem variar dependendo da região.

Como funcionam as APIs com atributos

As GuardDuty APIs continuarão retornando um `dataSources` objeto, conforme aplicável, e também retornarão um `features` objeto contendo as mesmas informações em um formato diferente. GuardDuty recursos lançados antes de março de 2023 estarão disponíveis por meio de `dataSources` objeto e `features` objeto. GuardDuty recursos lançados desde março de 2023 só estarão disponíveis por meio do `features` objeto. Você não pode criar ou atualizar um detector nem descrever seu AWS Organizations uso `dataSources` e a notação de `features` objeto na mesma solicitação de API. Para ativar os tipos de GuardDuty proteção, você precisará migrar suas fontes de dados existentes para o `features` objeto usando as mesmas APIs que agora também incluem o `features` objeto.

> **Note**
>
> GuardDuty não adicionará uma nova fonte de dados após essa modificação.

GuardDuty desaprovou o uso de fontes de dados associadas aos planos de proteção. No entanto, ele ainda é compatível com GuardDuty fontes de dados fundamentais. As GuardDuty melhores práticas recomendam o uso de recursos para ativar ou editar a configuração de qualquer plano de proteção em sua conta.

Como incorporar alterações de atributos nas APIs

- Se você gerencia GuardDuty configurações por meio de APIs, SDKs ou CloudFormation modelo e deseja habilitar possíveis novos GuardDuty recursos, precisará modificar seu código e modelo, respectivamente. Para obter mais informações, consulte as APIs atualizadas na Amazon GuardDuty API Reference.
- Para GuardDuty recursos configurados antes dessa atualização, você pode continuar usando as APIs, os SDKs ou CloudFormation o modelo. No entanto, recomendamos que se passe a usar o objeto `feature`.

  Todas as fontes de dados têm um objeto de atributo equivalente. Para obter mais informações, consulte Como mapear `dataSources` para `features`.
- Atualmente, `additionalConfiguration` o objeto `features` está disponível apenas para determinados tipos de proteção.

- Para esses tipos de proteção, se o seu recurso `AdditionalConfiguration` `status` estiver definido como`ENABLED`, mas a configuração do seu recurso não `status` estiver definida`ENABLED`, não GuardDuty tomará nenhuma ação nesse caso.
- As seguintes APIs são afetadas por isso:
  - UpdateDetector
  - UpdateMemberDetectors
  - UpdateOrganizationConfiguration

Como mapear **`dataSources`** para **`features`**

A tabela a seguir mostra o mapeamento dos tipos de proteção, `dataSources`, e `features`.

GuardDuty tipo de proteção	Nome da fonte de dados *	Nome do atributo
Logs de fluxo da VPC	`flowLogs` (somente leitura, não pode ser modificado)	`FLOW_LOGS` (somente leitura, não pode ser modificado)
Logs de consultas de DNS do Route53 Resolver	`dnsLogs` (somente leitura, não pode ser modificado)	`DNS_LOGS` (somente leitura, não pode ser modificado)
CloudTrail eventos	`cloudTrail` (somente leitura, não pode ser modificado)	`CLOUD_TRAIL` (somente leitura, não pode ser modificado)
S3	`s3Logs`	`S3_DATA_EVENTS`
Proteção do EKS	`kubernetes.auditlogs`	`EKS_AUDIT_LOGS`
Proteção contra malware para o S3	`malwareProtection.scanEc2InstanceWithFindings.ebsVolumes`	`EBS_MALWARE_PROTECTION`

GuardDuty tipo de proteção	Nome da fonte de dados *	Nome do atributo
Eventos de login do RDS	GuardDuty fornece suporte somente à ativação de recursos para esses tipos de proteção.	`RDS_LOGIN_EVENTS`
Monitoramento de runtime do EKS		`EKS_RUNTIME_MONITORING`
Monitoramento de runtime		`RUNTIME_MONITORING`

GuardDuty agente de segurança para clusters Amazon EKS		`EKS_RUNTIME_MONITORING.additionalConfiguration.EKS_ADDON_MANAGEMENT`
		
		`RUNTIME_MONITORING.additionalConfiguration.EKS_ADDON_MANAGEMENT`

GuardDuty agente de segurança para ECS-Fargate clusters da Amazon		`RUNTIME_MONITORING.additionalConfiguration.ECS_FARGATE_AGENT_MANAGEMENT`

GuardDuty tipo de proteção	Nome da fonte de dados *	Nome do atributo
GuardDuty agente de segurança para instâncias do Amazon EC2		`RUNTIME_MONITORING.additionalConfiguration.EC2_AGENT_MANAGEMENT`
Proteção do Lambda		`LAMBDA_NETWORK_LOGS`

*GetUsageStatistics usa seus próprios nomes de `dataSource`. Para acessar mais informações, consulte Monitorando GuardDuty o uso e estimando custos ou GetUsageStatistics.

Segurança na Amazon GuardDuty

A segurança na nuvem AWS é a maior prioridade. Como AWS cliente, você se beneficia de uma arquitetura de data center e rede criada para atender aos requisitos das organizações mais sensíveis à segurança.

A segurança é uma responsabilidade compartilhada entre você AWS e você. O modelo de responsabilidade compartilhada descreve isso como a segurança da nuvem e a segurança na nuvem:

- Segurança da nuvem — AWS é responsável por proteger a infraestrutura que executa AWS os serviços na AWS nuvem. AWS também fornece serviços que você pode usar com segurança. Third-party auditores testam e verificam regularmente a eficácia de nossa segurança como parte dos programas de AWS conformidade dos programas de de . Para saber mais sobre os programas de conformidade que se aplicam a GuardDuty, consulte AWS serviços no escopo por programa de conformidade AWS .
- Segurança na nuvem — Sua responsabilidade é determinada pelo AWS serviço que você usa. Você também é responsável por outros fatores, incluindo a confidencialidade de seus dados, os requisitos da sua empresa e as leis e normas aplicáveis.

Esta documentação ajuda você a entender como aplicar o modelo de responsabilidade compartilhada ao usar GuardDuty. Ele mostra como configurar para atender GuardDuty aos seus objetivos de segurança e conformidade. Você também aprenderá a usar outros AWS serviços que ajudam a monitorar e proteger seus GuardDuty recursos.

Conteúdo

- Proteção de dados na Amazon GuardDuty
- Registrando chamadas de GuardDuty API da Amazon com AWS CloudTrail
- Identity and Access Management para Amazon GuardDuty
- Validação de conformidade para a Amazon GuardDuty
- Resiliência na Amazon GuardDuty
- Segurança da infraestrutura na Amazon GuardDuty
- Amazon GuardDuty e endpoints VPC de interface ()AWS PrivateLink

Proteção de dados na Amazon GuardDuty

O modelo de responsabilidade AWS https://aws.amazon.com/compliance/shared-responsibility-model/ se aplica à proteção de dados na Amazon GuardDuty. Conforme descrito neste modelo, AWS é responsável por proteger a infraestrutura global que opera todos os Nuvem AWS. Você é responsável por manter o controle sobre o conteúdo hospedado nessa infraestrutura. Você também é responsável pelas tarefas de configuração e gerenciamento de segurança dos Serviços da AWS que usa. Para obter mais informações sobre privacidade de dados, consulte Perguntas frequentes sobre privacidade de dados e termos AWS da região da China. Para obter informações sobre proteção de dados na Europa, consulte o Centro de Regulamento Geral sobre a Proteção de Dados (RGPD).

Para fins de proteção de dados, recomendamos que você proteja Conta da AWS as credenciais e configure usuários individuais com Centro de Identidade do AWS IAM ou AWS Identity and Access Management (IAM). Dessa maneira, cada usuário receberá apenas as permissões necessárias para cumprir suas obrigações de trabalho. Recomendamos também que você proteja seus dados das seguintes formas:

- Use uma autenticação multifator (MFA) com cada conta.
- Use SSL/TLS para se comunicar com AWS recursos. Exigimos TLS 1.2 e recomendamos TLS 1.3.
- Configure a API e o registro de atividades do usuário com AWS CloudTrail. Para obter informações sobre como usar CloudTrail trilhas para capturar AWS atividades, consulte Como trabalhar com CloudTrail trilhas no Guia AWS CloudTrail do usuário.
- Use soluções AWS de criptografia, junto com todos os controles de segurança padrão Serviços da AWS.
- Use serviços gerenciados de segurança avançada, como o Amazon Macie, que ajuda a localizar e proteger dados sensíveis armazenados no Amazon S3.
- Se você precisar de módulos criptográficos validados pelo FIPS 140-3 ao acessar AWS por meio de uma interface de linha de comando ou de uma API, use um endpoint FIPS. Para saber mais sobre os endpoints FIPS disponíveis, consulte Federal Information Processing Standard (FIPS) 140-3.

É altamente recomendável que nunca sejam colocadas informações confidenciais ou sensíveis, como endereços de e-mail de clientes, em tags ou campos de formato livre, como um campo Nome. Isso inclui quando você trabalha com GuardDuty ou com outras pessoas Serviços da AWS usando o console, a API ou AWS os SDKs. AWS CLI Quaisquer dados inseridos em tags ou em campos

de texto de formato livre usados para nomes podem ser usados para logs de faturamento ou de diagnóstico. Se você fornecer um URL para um servidor externo, é fortemente recomendável que não sejam incluídas informações de credenciais no URL para validar a solicitação nesse servidor.

Criptografia em repouso

Todos os dados GuardDuty do cliente são criptografados em repouso usando soluções AWS de criptografia.

GuardDuty dados, como descobertas, são criptografados em repouso usando AWS Key Management Service (AWS KMS) com chaves AWS próprias.

Criptografia em trânsito

GuardDuty analisa dados de log de outros serviços. O GuardDuty criptografa todos os dados em trânsito desses serviços com HTTPS e KMS. Depois de GuardDuty extrair as informações necessárias dos registros, elas são descartadas. Para obter mais informações sobre como GuardDuty usa as informações de outros serviços, consulte fontes GuardDuty de dados.

GuardDuty os dados são criptografados em trânsito entre os serviços.

Optar por não usar seus dados para melhorar o serviço

Você pode optar por não ter seus dados usados para desenvolver GuardDuty e melhorar outros serviços AWS de segurança usando a política de AWS Organizations exclusão. Você pode optar por não participar, mesmo GuardDuty que atualmente não colete esses dados. Para obter mais informações sobre como optar por não participar, consulte as políticas de exclusão dos serviços de IA no Guia do usuário do AWS Organizations .

> **Note**
>
> Para que você use a política de exclusão, suas AWS contas devem ser gerenciadas centralmente pelo. AWS Organizations Se você ainda não criou uma organização para suas AWS contas, consulte Criação e gerenciamento de uma organização no Guia do AWS Organizations usuário.

A exclusão tem os seguintes efeitos:

- GuardDuty excluirá os dados coletados e armazenados para fins de melhoria do serviço antes de sua exclusão (se houver).
- Depois de optar por não participar, não GuardDuty coletaremos nem armazenaremos mais esses dados para fins de melhoria do serviço.

Os tópicos a seguir explicam como cada recurso interno GuardDuty potencialmente manipula seus dados para melhorar o serviço.

Conteúdo

- GuardDuty Monitoramento da execução
- GuardDuty Proteção contra malware

GuardDuty Monitoramento da execução

GuardDuty O monitoramento de tempo de execução fornece detecção de ameaças em tempo de execução para clusters do Amazon Elastic Kubernetes Service (Amazon EKS), somente do AWS Fargate Amazon Elastic Container Service (Amazon ECS) e instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em seu ambiente. AWS Depois de ativar o Runtime Monitoring e implantar o agente de GuardDuty segurança para seu recurso, GuardDuty começa a monitorar e analisar os eventos de tempo de execução associados ao seu recurso. Esses tipos de eventos de runtime incluem eventos de processo, eventos de contêiner, eventos de DNS e muito mais. Para obter mais informações, consulte Tipos de eventos de tempo de execução coletados que GuardDuty usam.

GuardDuty coleta os comandos (como `curl`, `systemctl`, `ecron`) e seus argumentos associados (como `start`, `stop`, `disable`) de suas cargas de trabalho. Por exemplo, quando alguém executa `systemctl stop` *`service-name`*, GuardDuty captura o comando `systemctl` e seus argumentos `stop` *`service-name`*. Essas informações detalhadas ajudam GuardDuty a detectar ameaças sofisticadas analisando padrões de comando e correlacionando vários eventos. Por exemplo, GuardDuty pode identificar quando um invasor tenta desativar os serviços de segurança ou executa arquivos maliciosos conhecidos. Embora use GuardDuty ativamente esses dados para detecção de ameaças, atualmente não usa esses comandos e argumentos para fins de aprimoramento do serviço (talvez o faça no futuro). Sua confiança, privacidade e segurança de seu conteúdo são nossa maior prioridade e garantem que nosso uso esteja em conformidade com nossos compromissos com você. Para obter mais informações, consulte Perguntas frequentes sobre a privacidade de dados.

GuardDuty Proteção contra malware

GuardDuty A proteção contra malware verifica e detecta malwares contidos em volumes do EBS vinculados às suas cargas de trabalho de instância e contêiner do Amazon EC2 potencialmente comprometidas, arquivos recém-carregados em seus buckets selecionados do Amazon S3 e recursos de backup. Atualmente, GuardDuty não coleta nem usa malware detectado para melhorar o serviço. No entanto, no futuro, quando o GuardDuty Malware Protection identificar um arquivo de volume do EBS, um arquivo de backup ou um arquivo S3 como malicioso ou prejudicial, o GuardDuty Malware Protection coletará e armazenará esse arquivo para desenvolver e melhorar suas detecções de malware e o serviço. GuardDuty Esse arquivo também pode ser usado para desenvolver e melhorar outros serviços de segurança da AWS . Sua confiança, privacidade e segurança de seu conteúdo são nossa maior prioridade e garantem que nosso uso esteja em conformidade com nossos compromissos com você. Para obter mais informações, consulte Perguntas frequentes sobre a privacidade de dados.

Registrando chamadas de GuardDuty API da Amazon com AWS CloudTrail

GuardDuty A Amazon está integrada com AWS CloudTrail, um serviço que fornece um registro das ações realizadas por um usuário, função ou AWS serviço em GuardDuty. CloudTrail captura todas as chamadas de API para GuardDuty eventos As, incluindo chamadas do GuardDuty console e de chamadas de código para as GuardDuty APIs. Se você criar uma trilha, poderá habilitar a entrega contínua de CloudTrail eventos para um bucket do Amazon Simple Storage Service (Amazon S3), incluindo eventos para. GuardDuty Se você não configurar uma trilha, ainda poderá ver os eventos mais recentes no CloudTrail console no Histórico de eventos. Usando as informações coletadas por CloudTrail, você pode determinar a solicitação que foi feita GuardDuty, o endereço IP do qual a solicitação foi feita, quem fez a solicitação, quando ela foi feita e detalhes adicionais.

Para obter mais informações sobre CloudTrail, inclusive como configurá-lo e ativá-lo, consulte o Guia AWS CloudTrail do usuário.

GuardDuty informações em CloudTrail

CloudTrail é ativado em sua AWS conta quando você cria a conta. Quando uma atividade de evento suportada ocorre em GuardDuty, essa atividade é registrada em um CloudTrail evento junto com outros eventos AWS de serviço no histórico de eventos. Você pode visualizar, pesquisar e baixar eventos recentes em sua AWS conta. Para obter mais informações, consulte Visualização de eventos com histórico de CloudTrail eventos.

Para um registro contínuo dos eventos em sua AWS conta, incluindo eventos para GuardDuty, crie uma trilha. Uma trilha permite CloudTrail entregar arquivos de log para um bucket do Amazon S3. Por padrão, quando uma trilha é criada no console, a mesma é aplicada a todas as regiões da . A trilha registra eventos de todas as regiões na AWS partição e entrega os arquivos de log ao bucket do Amazon S3 que você especificar. Além disso, você pode configurar outros AWS serviços para analisar e agir com base nos dados de eventos coletados nos CloudTrail registros. Para obter mais informações, consulte:

- Visão geral da criação de uma trilha
- Serviços e integrações compatíveis com o CloudTrail
- Configurando notificações do Amazon SNS para CloudTrail
- Recebendo arquivos de CloudTrail log de várias regiões e Recebendo arquivos de CloudTrail log de várias contas

Cada entrada de log ou evento contém informações sobre quem gerou a solicitação. As informações de identidade ajudam a determinar o seguinte:

- Se a solicitação foi feita com credenciais login de usuário raiz ou de usuário do IAM.
- Se a solicitação foi feita com credenciais de segurança temporárias de um perfil ou de um usuário federado
- Se a solicitação foi feita por outro AWS serviço

Para obter mais informações, consulte Elemento userIdentity do CloudTrail .

GuardDuty eventos do plano de controle em CloudTrail

Por padrão, CloudTrail registra todas as operações de GuardDuty API fornecidas na Amazon GuardDuty API Reference como eventos em CloudTrail arquivos.

GuardDuty eventos de dados em CloudTrail

GuardDuty Monitoramento de execuçãousa um agente de GuardDuty segurança implantado em seus clusters do Amazon Elastic Kubernetes Service (Amazon EKS), instâncias do Amazon Elastic Compute Cloud (Amazon EC2) e `aws-guardduty-agent` tarefas (somente Amazon AWS Fargate Elastic Container Service (Amazon ECS)) para coletar Tipos de eventos de runtime coletados complementos () que coletam para suas cargas de trabalho e, em seguida, enviá-las para detecção de ameaças e análise. AWS GuardDuty

Registro em log e monitoramento de eventos de dados

Opcionalmente, você pode configurar os AWS CloudTrail registros para visualizar os eventos de dados do seu agente GuardDuty de segurança.

Para criar e configurar CloudTrail, consulte Eventos de dados no Guia do AWS CloudTrail usuário e siga as instruções para registrar eventos de dados com seletores de eventos avançados no Console de gerenciamento da AWS. Ao registrar a trilha em log, faça as seguintes alterações:

- Para o tipo de evento de dados, escolha GuardDutydetector.
- Para o Modelo do seletor de logs, escolha Registrar todos os eventos em log.
- Expanda a Visualização JSON da configuração. Ela deve ser semelhante ao seguinte JSON:

```
[
  {
    "name": "",
    "fieldSelectors": [
      {
        "field": "eventCategory",
        "equals": [
          "Data"
        ]
      },
      {
        "field": "resources.type",
        "equals": [
          "AWS::GuardDuty::Detector"
        ]
      }
    ]
  }
]
```

Depois de habilitar o seletor para a trilha, navegue até o console do Amazon S3 em. https://console.aws.amazon.com/s3/ Você pode baixar os eventos de dados do bucket do S3 escolhido no momento da configuração dos CloudTrail registros.

Exemplo: entradas do arquivo de GuardDuty log

Uma trilha é uma configuração que permite a entrega de eventos como arquivos de log para um bucket do Amazon S3 que você especificar. CloudTrail os arquivos de log contêm uma ou mais entradas de log. Um evento representa uma única solicitação de qualquer fonte e inclui informações sobre a ação solicitada, a data e a hora da ação, os parâmetros da solicitação e assim por diante. CloudTrail os arquivos de log não são um rastreamento de pilha ordenado das chamadas públicas de API, portanto, eles não aparecem em nenhuma ordem específica.

O exemplo a seguir mostra uma entrada de CloudTrail registro que demonstra o evento do plano de dados.


```
{
        "eventVersion": "1.08",
        "userIdentity": {
            "type": "AssumedRole",
            "principalId": "111122223333:aws:ec2-instance:i-123412341234example",
            "arn": "arn:aws:sts::111122223333:assumed-role/aws:ec2-
instance/i-123412341234example",
            "accountId": "111122223333",
            "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
            "sessionContext": {
                "sessionIssuer": {
                    "type": "Role",
                    "principalId": "111122223333:aws:ec2-instance",
                    "arn": "arn:aws:iam::111122223333:role/aws:ec2-instance",
                    "accountId": "111122223333",
                    "userName": "aws:ec2-instance"
                },
                "attributes": {
                    "creationDate": "2023-03-05T04:00:21Z",
                    "mfaAuthenticated": "false"
                },
                "ec2RoleDelivery": "2.0"
            }
        },
        "eventTime": "2023-03-05T06:03:49Z",
        "eventSource": "guardduty.amazonaws.com",
        "eventName": "SendSecurityTelemetry",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "54.240.230.177",
        "userAgent": "aws-sdk-rust/0.54.1 os/linux lang/rust/1.66.0",
```

```
        "requestParameters": null,
        "responseElements": null,
        "requestID": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
        "eventID": "a1b2c3d4-5678-90ab-cdef-EXAMPLEbbbbb",
        "readOnly": false,
        "resources": [{
            "accountId": "111122223333",
            "type": "AWS::GuardDuty::Detector",
            "ARN": "arn:aws:guardduty:us-
west-2:111122223333:detector/12abc34d567e8fa901bc2d34e56789f0"
        }],
        "eventType": "AwsApiCall",
        "managementEvent": false,
        "recipientAccountId": "111122223333",
        "eventCategory": "Data",
        "tlsDetails": {
            "tlsVersion": "TLSv1.2",
            "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
            "clientProvidedHostHeader": "guardduty-data.us-east-1.amazonaws.com"
        }
    }
```

O exemplo a seguir mostra uma entrada de CloudTrail registro que demonstra a `CreateIPThreatIntelSet` ação (evento do plano de controle).

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::444455556666:user/Alice",
        "accountId": "444455556666",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "sessionContext": {
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2018-06-14T22:54:20Z"
            },
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                "arn": "arn:aws:iam::444455556666:user/Alice",
                "accountId": "444455556666",
```

```
                "userName": "Alice"
            }
        }
    },
    "eventTime": "2018-06-14T22:57:56Z",
    "eventSource": "guardduty.amazonaws.com",
    "eventName": "CreateThreatIntelSet",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "54.240.230.177",
    "userAgent": "console.amazonaws.com",
    "requestParameters": {
        "detectorId": "12abc34d567e8fa901bc2d34e56789f0",
        "name": "Example",
        "format": "TXT",
        "activate": false,
        "location": "https://s3.amazonaws.com/bucket.name/file.txt"
    },
    "responseElements": {
        "threatIntelSetId": "1ab200428351c99d859bf61992460d24"
    },
    "requestID": "5f6bf981-7026-11e8-a9fc-5b37d2684c5c",
    "eventID": "81337b11-e5c8-4f91-b141-deb405625bc9",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "recipientAccountId": "444455556666"
}
```


A partir das informações desse evento, você pode determinar que a solicitação foi feita para criar uma lista de ameaças `Example` no GuardDuty. Você também pode ver que a solicitação foi feita por uma usuária chamada Alice em 14 de junho de 2018.

Identity and Access Management para Amazon GuardDuty

AWS Identity and Access Management (IAM) é uma ferramenta AWS service (Serviço da AWS) que ajuda o administrador a controlar com segurança o acesso aos AWS recursos. Os administradores do IAM controlam quem pode ser autenticado (conectado) e autorizado (tem permissões) a usar GuardDuty os recursos. O IAM é um AWS service (Serviço da AWS) que você pode usar sem custo adicional.

Tópicos

- Público
- Autenticação com identidades
- Gerenciar o acesso usando políticas
- Como a Amazon GuardDuty trabalha com o IAM
- Identity-based exemplos de políticas para a Amazon GuardDuty
- Usando funções vinculadas a serviços para a Amazon GuardDuty
- AWS políticas gerenciadas para a Amazon GuardDuty
- Solução de problemas de GuardDuty identidade e acesso da Amazon

Público

A forma como você usa AWS Identity and Access Management (IAM) difere com base na sua função:

- Usuário do serviço: solicite permissões ao seu administrador se você não conseguir acessar os atributos (consulte Solução de problemas de GuardDuty identidade e acesso da Amazon).
- Administrador do serviço: determine o acesso do usuário e envie solicitações de permissão (consulte Como a Amazon GuardDuty trabalha com o IAM)
- Administrador do IAM: escreva políticas para gerenciar o acesso (consulte Identity-based exemplos de políticas para a Amazon GuardDuty)

Autenticação com identidades

A autenticação é a forma como você faz login AWS usando suas credenciais de identidade. Você deve estar autenticado como usuário do IAM ou assumindo uma função do IAM. Usuário raiz da conta da AWS

Você pode fazer login como uma identidade federada usando credenciais de uma fonte de identidade como Centro de Identidade do AWS IAM (IAM Identity Center), autenticação de login único ou credenciais. Google/Facebook Para ter mais informações sobre como fazer login, consulte Como fazer login em sua Conta da AWS no Guia do usuário do Início de Sessão da AWS .

Para acesso programático, AWS fornece um SDK e uma CLI para assinar solicitações criptograficamente. Para ter mais informações, consulte AWS Signature Version 4 para solicitações de API no Guia do usuário do IAM.

Conta da AWS usuário-raiz

Ao criar um Conta da AWS, você começa com uma identidade de login chamada usuário Conta da AWS raiz que tem acesso completo a todos Serviços da AWS os recursos. É altamente recomendável não usar o usuário-raiz em tarefas diárias. Consulte as tarefas que exigem credenciais de usuário-raiz em Tarefas que exigem credenciais de usuário-raiz no Guia do usuário do IAM.

Identidade federada

Como prática recomendada, exija que os usuários humanos usem a federação com um provedor de identidade para acessar Serviços da AWS usando credenciais temporárias.

Uma identidade federada é um usuário do seu diretório corporativo, provedor de identidade da web ou Directory Service que acessa Serviços da AWS usando credenciais de uma fonte de identidade. As identidades federadas assumem funções que oferecem credenciais temporárias.

Para o gerenciamento de acesso centralizado, recomendamos Centro de Identidade do AWS IAM. Para saber mais, consulte O que é o IAM Identity Center? no Guia do usuário do Centro de Identidade do AWS IAM .

Usuários e grupos do IAM

Um usuário do IAM é uma identidade com permissões específicas para uma única pessoa ou aplicação. É recomendável usar credenciais temporárias, em vez de usuários do IAM com credenciais de longo prazo. Para obter mais informações, consulte Exigir que usuários humanos usem a federação com um provedor de identidade para acessar AWS usando credenciais temporárias no Guia do usuário do IAM.

Um grupo do IAM especifica um conjunto de usuários do IAM e facilita o gerenciamento de permissões para grandes conjuntos de usuários. Para ter mais informações, consulte Casos de uso de usuários do IAM no Guia do usuário do IAM.

Perfis do IAM

Uma perfil do IAM é uma identidade com permissões específicas que oferece credenciais temporárias. Você pode assumir uma função mudando de um usuário para uma função do IAM (console) ou chamando uma operação de AWS API AWS CLI ou. Para saber mais, consulte Métodos para assumir um perfil no Manual do usuário do IAM.

Os perfis do IAM são úteis para acesso de usuário federado, permissões de usuário do IAM temporárias, acesso entre contas, acesso entre serviços e aplicações em execução no Amazon EC2. Consulte mais informações em Acesso a recursos entre contas no IAM no Guia do usuário do IAM.

Gerenciar o acesso usando políticas

Você controla o acesso AWS criando políticas e anexando-as a AWS identidades ou recursos. Uma política define permissões quando associada a uma identidade ou recurso. AWS avalia essas políticas quando um diretor faz uma solicitação. A maioria das políticas é armazenada AWS como documentos JSON. Para ter mais informações sobre documentos de política JSON, consulte Visão geral das políticas JSON no Guia do usuário do IAM.

Por meio de políticas, os administradores especificam quem tem acesso a que, definindo qual entidade principal pode realizar ações em quais recursos e sob quais condições.

Por padrão, usuários e perfis não têm permissões. Um administrador do IAM cria políticas do IAM e as adiciona aos perfis, os quais os usuários podem então assumir. As políticas do IAM definem permissões, independentemente do método usado para realizar a operação.

Identity-based políticas

Identity-based políticas são documentos de políticas de permissões JSON que você anexa a uma identidade (usuário, grupo ou função). Essas políticas controlam quais ações as identidades podem realizar, em quais recursos e sob quais condições. Para saber como criar uma política baseada em identidade, consulte Definir permissões personalizadas do IAM com as políticas gerenciadas pelo cliente no Guia do Usuário do IAM.

Identity-based as políticas podem ser políticas em linha (incorporadas diretamente em uma única identidade) ou políticas gerenciadas (políticas autônomas anexadas a várias identidades). Para saber como escolher entre uma política gerenciada e políticas em linha, consulte Escolher entre políticas gerenciadas e políticas em linha no Guia do usuário do IAM.

Resource-based políticas

Resource-based políticas são documentos de política JSON que você anexa a um recurso. Entre os exemplos estão políticas de confiança de perfil do IAM e políticas de bucket do Amazon S3. Em serviços compatíveis com políticas baseadas em recursos, os administradores de serviço podem usá-las para controlar o acesso a um recurso específico. É necessário especificar uma entidade principal em uma política baseada em recursos.

Resource-based as políticas são políticas em linha localizadas nesse serviço. Você não pode usar políticas AWS gerenciadas do IAM em uma política baseada em recursos.

Outros tipos de política

AWS oferece suporte a tipos de políticas adicionais que podem definir o máximo de permissões concedidas por tipos de políticas mais comuns:

- Limites de permissões: definem o número máximo de permissões que uma política baseada em identidade pode conceder a uma entidade do IAM. Para saber mais sobre limites de permissões, consulte Limites de permissões para identidades do IAM no Guia do usuário do IAM.
- Políticas de Controle de Serviços (SCPs): as SCPs especificam o número máximo de permissões para uma organização ou uma unidade organizacional no AWS Organizations. Para saber mais, consulte Políticas de controle de serviço no Guia do usuário do AWS Organizations .
- Políticas de controle de recursos (RCPs): definem o número máximo de permissões disponíveis para recursos em suas contas. Consulte mais informações em Resource control policies (RCPs) no Guia do usuário do AWS Organizations .
- Políticas de sessão: políticas avançadas transmitidas como um parâmetro durante a criação de uma sessão temporária para um perfil ou um usuário federado. Para saber mais, consulte Políticas de sessão no Guia do usuário do IAM.

Vários tipos de política

Quando vários tipos de política são aplicáveis a uma solicitação, é mais complicado compreender as permissões resultantes. Para saber como AWS determinar se uma solicitação deve ser permitida quando vários tipos de políticas estão envolvidos, consulte Lógica de avaliação de políticas no Guia do usuário do IAM.

Como a Amazon GuardDuty trabalha com o IAM

Antes de usar o IAM para gerenciar o acesso GuardDuty, saiba com quais recursos do IAM estão disponíveis para uso GuardDuty.

Recursos do IAM que você pode usar com a Amazon GuardDuty

Recurso do IAM	GuardDuty apoio
Identity-based políticas	Sim
Resource-based políticas	Não
Ações de políticas	Sim
Recursos de políticas	Sim
Chaves de condição de políticas	Sim
ACLs	Não
ABAC (tags em políticas)	Parcial
Credenciais temporárias	Sim
Permissões de entidade principal	Sim
Perfis de serviço	Sim
Service-linked funções	Sim

Para ter uma visão de alto nível de como GuardDuty e outros AWS serviços funcionam com a maioria dos recursos do IAM, consulte AWS os serviços que funcionam com o IAM no Guia do usuário do IAM.

Identity-based políticas para GuardDuty

Compatível com políticas baseadas em identidade: sim

Identity-based políticas são documentos de políticas de permissões JSON que você pode anexar a uma identidade, como um usuário do IAM, um grupo de usuários ou uma função. Essas políticas controlam quais ações os usuários e perfis podem realizar, em quais atributos e em que condições. Para saber como criar uma política baseada em identidade, consulte Definir permissões personalizadas do IAM com as políticas gerenciadas pelo cliente no Guia do Usuário do IAM.

Com as políticas baseadas em identidade do IAM, é possível especificar ações e recursos permitidos ou negados, assim como as condições sob as quais as ações são permitidas ou negadas. Para saber mais sobre todos os elementos que podem ser usados em uma política JSON, consulte Referência de elemento de política JSON do IAM no Guia do usuário do IAM.

Identity-based exemplos de políticas para GuardDuty

Para ver exemplos de políticas GuardDuty baseadas em identidade, consulte. Identity-based exemplos de políticas para a Amazon GuardDuty

Resource-based políticas dentro GuardDuty

Compatibilidade com políticas baseadas em recursos: não

Resource-based políticas são documentos de política JSON que você anexa a um recurso. São exemplos de políticas baseadas em recursos as políticas de confiança de perfil do IAM e as políticas de bucket do Amazon S3. Em serviços compatíveis com políticas baseadas em recursos, os administradores de serviço podem usá-las para controlar o acesso a um recurso específico. Para o atributo ao qual a política está anexada, a política define quais ações uma entidade principal especificado pode executar nesse atributo e em que condições. É necessário especificar uma entidade principal em uma política baseada em recursos. Os diretores podem incluir contas, usuários, funções, usuários federados ou. Serviços da AWS

Para permitir o acesso entre contas, é possível especificar uma conta inteira ou as entidades do IAM em outra conta como a entidade principal em uma política baseada em recursos. Consulte mais informações em Acesso a recursos entre contas no IAM no Guia do usuário do IAM.

Ações políticas para GuardDuty

Compatível com ações de políticas: sim

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

O elemento `Action` de uma política JSON descreve as ações que podem ser usadas para permitir ou negar acesso em uma política. Incluem ações em uma política para conceder permissões para executar a operação associada.

Para ver uma lista de GuardDuty ações, consulte Ações definidas pela Amazon GuardDuty na Referência de autorização de serviço.

As ações de política GuardDuty usam o seguinte prefixo antes da ação:

```
guardduty
```

Para especificar várias ações em uma única declaração, separe-as com vírgulas.

```
"Action": [
      "guardduty:action1",
      "guardduty:action2"
         ]
```

Para ver exemplos de políticas GuardDuty baseadas em identidade, consulte. Identity-based exemplos de políticas para a Amazon GuardDuty

Recursos políticos para GuardDuty

Compatível com recursos de políticas: sim

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

O elemento de política JSON `Resource` especifica o objeto ou os objetos aos quais a ação se aplica. Como prática recomendada, especifique um recurso usando seu nome do recurso da Amazon (ARN). Para ações que não oferecem compatibilidade com permissões em nível de recurso, use um curinga (*) para indicar que a instrução se aplica a todos os recursos.

```
"Resource": "*"
```

Para ver uma lista dos tipos de GuardDuty recursos e seus ARNs, consulte Recursos definidos pela Amazon GuardDuty na Referência de autorização de serviço. Para saber com quais ações você pode especificar o ARN de cada recurso, consulte Ações definidas pela Amazon. GuardDuty

Para ver exemplos de políticas GuardDuty baseadas em identidade, consulte. Identity-based exemplos de políticas para a Amazon GuardDuty

Chaves de condição de política para GuardDuty

Compatível com chaves de condição de política específicas de serviço: sim

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

O elemento `Condition` especifica quando as instruções são executadas com base em critérios definidos. É possível criar expressões condicionais que usem agentes de condição, como “igual a” ou “menor que”, para fazer a condição da política corresponder aos valores na solicitação. Para ver todas as chaves de condição AWS globais, consulte as chaves de contexto de condição AWS global no Guia do usuário do IAM.

Para ver uma lista de chaves de GuardDuty condição, consulte Chaves de condição da Amazon GuardDuty na Referência de autorização de serviço. Para saber com quais ações e recursos você pode usar uma chave de condição, consulte Ações definidas pela Amazon GuardDuty.

Para ver exemplos de políticas GuardDuty baseadas em identidade, consulte. Identity-based exemplos de políticas para a Amazon GuardDuty

Listas de controle de acesso (ACLs) em GuardDuty

Compatível com ACLs: não

As listas de controle de acesso (ACLs) controlam quais entidades principais (membros, usuários ou perfis da conta) têm permissões para acessar um recurso. As ACLs são semelhantes às políticas baseadas em recursos, embora não usem o formato de documento de política JSON.

Attribute-based controle de acesso (ABAC) com GuardDuty

Compatível com ABAC (tags em políticas): parcial

Attribute-based controle de acesso (ABAC) é uma estratégia de autorização que define permissões com base em atributos chamados de tags. Você pode anexar tags a entidades e AWS recursos do IAM e, em seguida, criar políticas ABAC para permitir operações quando a tag do diretor corresponder à tag no recurso.

Para controlar o acesso baseado em tags, forneça informações sobre as tags no elemento de condição de uma política usando as `aws:ResourceTag/`*`key-name`*, `aws:RequestTag/`*`key-name`* ou chaves de condição `aws:TagKeys`.

Se um serviço for compatível com as três chaves de condição para cada tipo de recurso, o valor será Sim para o serviço. Se um serviço for compatível com as três chaves de condição somente para alguns tipos de recursos, o valor será Parcial

Para saber mais sobre o ABAC, consulte Definir permissões com autorização do ABAC no Guia do usuário do IAM. Para visualizar um tutorial com etapas para configurar o ABAC, consulte Usar controle de acesso por atributo (ABAC) no Guia do usuário do IAM.

Usando credenciais temporárias com GuardDuty

Compatível com credenciais temporárias: sim

As credenciais temporárias fornecem acesso de curto prazo aos AWS recursos e são criadas automaticamente quando você usa a federação ou troca de funções. AWS recomenda que você gere credenciais temporárias dinamicamente em vez de usar chaves de acesso de longo prazo. Para ter mais informações, consulte Credenciais de segurança temporárias no IAM e Serviços da Serviços da AWS que funcionam com o IAM no Guia do usuário do IAM.

Cross-service permissões principais para GuardDuty

Compatibilidade com o recurso de encaminhamento de sessões de acesso (FAS): sim

As sessões de acesso direto (FAS) usam as permissões do principal chamando um AWS service (Serviço da AWS), combinadas com a solicitação AWS service (Serviço da AWS) de fazer solicitações aos serviços posteriores. Para obter detalhes da política ao fazer solicitações de FAS, consulte Sessões de acesso direto.

Funções de serviço para GuardDuty

Compatível com perfis de serviço: sim

O perfil de serviço é um perfil do IAM que um serviço assume para executar ações em seu nome. Um administrador do IAM pode criar, modificar e excluir um perfil de serviço do IAM. Para saber mais, consulte Criar um perfil para delegar permissões a um AWS service (Serviço da AWS) no Guia do Usuário do IAM.

> **Warning**
>
> Alterar as permissões de uma função de serviço pode interromper GuardDuty a funcionalidade. Edite as funções de serviço somente quando GuardDuty fornecer orientação para fazer isso.

Service-linked funções para GuardDuty

Compatibilidade com perfis vinculados a serviços: sim

Uma função vinculada ao serviço é um tipo de função de serviço vinculada a um. AWS service (Serviço da AWS) O serviço pode assumir a função de realizar uma ação em seu nome. Service-linked as funções aparecem no seu Conta da AWS e são de propriedade do serviço. Um administrador do IAM pode visualizar, mas não editar as permissões para perfis vinculados ao serviço.

Para obter detalhes sobre como criar ou gerenciar funções GuardDuty vinculadas a serviços, consulte. Usando funções vinculadas a serviços para a Amazon GuardDuty

Para obter detalhes sobre como criar ou gerenciar perfis vinculados a serviços, consulte Serviços da AWS que funcionam com o IAM. Encontre um serviço na tabela que inclua um `Yes` na coluna de Service-linked função. Escolha o link Sim para visualizar a documentação do perfil vinculado a serviço desse serviço.

Identity-based exemplos de políticas para a Amazon GuardDuty

Por padrão, usuários e perfis não têm permissão para criar ou modificar recursos do GuardDuty. Para conceder permissão aos usuários para executar ações nos recursos que eles precisam, um administrador do IAM pode criar políticas do IAM.

Para aprender a criar uma política baseada em identidade do IAM ao usar esses documentos de política em JSON de exemplo, consulte Criar políticas do IAM (console) no Guia do usuário do IAM.

Para obter detalhes sobre ações e tipos de recursos definidos por GuardDuty, incluindo o formato dos ARNs para cada um dos tipos de recursos, consulte Ações, recursos e chaves de condição para a Amazon GuardDuty na Referência de Autorização de Serviço.

Tópicos

- Práticas recomendadas de política
- Usando o GuardDuty console
- Permissões necessárias para habilitar GuardDuty
- Permitir que os usuários visualizem suas próprias permissões
- Política personalizada do IAM para conceder acesso somente de leitura ao GuardDuty

- Negar acesso às GuardDuty descobertas
- Usando uma política personalizada do IAM para limitar o acesso aos GuardDuty recursos

Práticas recomendadas de política

Identity-based as políticas determinam se alguém pode criar, acessar ou excluir GuardDuty recursos em sua conta. Essas ações podem incorrer em custos para sua Conta da AWS. Ao criar ou editar políticas baseadas em identidade, siga estas diretrizes e recomendações:

- Comece com as políticas AWS gerenciadas e avance para as permissões de privilégios mínimos — Para começar a conceder permissões aos seus usuários e cargas de trabalho, use as políticas AWS gerenciadas que concedem permissões para muitos casos de uso comuns. Eles estão disponíveis no seu Conta da AWS. Recomendamos que você reduza ainda mais as permissões definindo políticas gerenciadas pelo AWS cliente que sejam específicas para seus casos de uso. Para saber mais, consulte Políticas gerenciadas pela AWS ou Políticas gerenciadas pela AWS para funções de trabalho no Guia do usuário do IAM.
- Aplique permissões de privilégio mínimo: ao definir permissões com as políticas do IAM, conceda apenas as permissões necessárias para executar uma tarefa. Você faz isso definindo as ações que podem ser executadas em recursos específicos sob condições específicas, também conhecidas como permissões de privilégio mínimo. Para saber mais sobre como usar o IAM para aplicar permissões, consulte Políticas e permissões no IAM no Guia do usuário do IAM.
- Use condições nas políticas do IAM para restringir ainda mais o acesso: é possível adicionar uma condição às políticas para limitar o acesso a ações e recursos. Por exemplo, é possível escrever uma condição de política para especificar que todas as solicitações devem ser enviadas usando SSL. Você também pode usar condições para conceder acesso às ações de serviço se elas forem usadas por meio de uma ação específica AWS service (Serviço da AWS), como CloudFormation. Para saber mais, consulte Elementos da política JSON do IAM: condição no Guia do usuário do IAM.
- Use o IAM Access Analyzer para validar suas políticas do IAM a fim de garantir permissões seguras e funcionais: o IAM Access Analyzer valida as políticas novas e existentes para que elas sigam a linguagem de política do IAM (JSON) e as práticas recomendadas do IAM. O IAM Access Analyzer oferece mais de cem verificações de política e recomendações práticas para ajudar a criar políticas seguras e funcionais. Para saber mais, consulte Validação de políticas do IAM Access Analyzer no Guia do Usuário do IAM.
- Exigir autenticação multifator (MFA) — Se você tiver um cenário que exija usuários do IAM ou um usuário root, ative Conta da AWS a MFA para obter segurança adicional. Para exigir MFA quando

as operações de API forem chamadas, adicione condições de MFA às suas políticas. Para saber mais, consulte Configuração de acesso à API protegido por MFA no Guia do Usuário do IAM.

Para saber mais sobre as práticas recomendadas do IAM, consulte Práticas recomendadas de segurança no IAM no Guia do usuário do IAM.

Usando o GuardDuty console

Para acessar o GuardDuty console da Amazon, você deve ter um conjunto mínimo de permissões. Essas permissões devem permitir que você liste e visualize detalhes sobre os GuardDuty recursos em seu Conta da AWS. Caso crie uma política baseada em identidade mais restritiva que as permissões mínimas necessárias, o console não funcionará como pretendido para entidades (usuários ou perfis) com essa política.

Você não precisa permitir permissões mínimas do console para usuários que estão fazendo chamadas somente para a API AWS CLI ou para a AWS API. Em vez disso, permita o acesso somente a ações que correspondam à operação de API que estiverem tentando executar.

Para garantir que usuários e funções ainda possam usar o GuardDuty console, anexe também a política GuardDuty `ConsoleAccess` ou a política `ReadOnly` AWS gerenciada às entidades. Para saber mais, consulte Adicionar permissões a um usuário no Guia do usuário do IAM.

Permissões necessárias para habilitar GuardDuty

Para conceder permissões que várias identidades do IAM (usuários, grupos e funções) devem ter, anexe a AWS política gerenciada: AmazonGuardDutyFullAccess_v2 (recomendado) política necessária para GuardDuty habilitar.

Permitir que os usuários visualizem suas próprias permissões

Este exemplo mostra como criar uma política que permita que os usuários do IAM visualizem as políticas gerenciadas e em linha anexadas a sua identidade de usuário. Essa política inclui permissões para concluir essa ação no console ou programaticamente usando a API AWS CLI ou AWS .

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
```

```
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Política personalizada do IAM para conceder acesso somente de leitura ao GuardDuty

Para conceder acesso somente de leitura, GuardDuty você pode usar a política `AmazonGuardDutyReadOnlyAccess` gerenciada.

Para criar uma política personalizada que conceda acesso somente para leitura a uma função, usuário ou grupo do IAM GuardDuty, você pode usar a seguinte declaração:

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
```

```
            "Effect": "Allow",
            "Action": [
                "guardduty:ListMembers",
                "guardduty:GetMembers",
                "guardduty:ListInvitations",
                "guardduty:ListDetectors",
                "guardduty:GetDetector",
                "guardduty:ListFindings",
                "guardduty:GetFindings",
                "guardduty:ListIPSets",
                "guardduty:GetIPSet",
                "guardduty:ListThreatIntelSets",
                "guardduty:GetThreatIntelSet",
                "guardduty:GetMasterAccount",
                "guardduty:GetInvitationsCount",
                "guardduty:GetFindingsStatistics",
                "guardduty:DescribeMalwareScans",
                "guardduty:UpdateMalwareScanSettings",
                "guardduty:GetMalwareScanSettings"
            ],
            "Resource": "*"
        }
    ]
}
```

Negar acesso às GuardDuty descobertas

Você pode usar a política a seguir para negar acesso às GuardDuty descobertas de uma função, usuário ou grupo do IAM. Os usuários não podem ver as descobertas ou os detalhes sobre as descobertas, mas podem acessar todas as outras GuardDuty operações:

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "guardduty:CreateDetector",
                "guardduty:DeleteDetector",
```

```
                "guardduty:UpdateDetector",
                "guardduty:GetDetector",
                "guardduty:ListDetectors",
                "guardduty:CreateIPSet",
                "guardduty:DeleteIPSet",
                "guardduty:UpdateIPSet",
                "guardduty:GetIPSet",
                "guardduty:ListIPSets",
                "guardduty:CreateThreatIntelSet",
                "guardduty:DeleteThreatIntelSet",
                "guardduty:UpdateThreatIntelSet",
                "guardduty:GetThreatIntelSet",
                "guardduty:ListThreatIntelSets",
                "guardduty:ArchiveFindings",
                "guardduty:UnarchiveFindings",
                "guardduty:CreateSampleFindings",
                "guardduty:CreateMembers",
                "guardduty:InviteMembers",
                "guardduty:GetMembers",
                "guardduty:DeleteMembers",
                "guardduty:DisassociateMembers",
                "guardduty:StartMonitoringMembers",
                "guardduty:StopMonitoringMembers",
                "guardduty:ListMembers",
                "guardduty:GetMasterAccount",
                "guardduty:DisassociateFromMasterAccount",
                "guardduty:AcceptAdministratorInvitation",
                "guardduty:ListInvitations",
                "guardduty:GetInvitationsCount",
                "guardduty:DeclineInvitations",
                "guardduty:DeleteInvitations"
            ],
            "Resource": "*"
        },
         {
            "Effect": "Allow",
            "Action": [
                "iam:CreateServiceLinkedRole"
            ],
            "Resource": "arn:aws:iam::123456789012:role/aws-service-role/
guardduty.amazonaws.com/AWSServiceRoleForAmazonGuardDuty",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "guardduty.amazonaws.com"
```

```
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:PutRolePolicy",
                "iam:DeleteRolePolicy"
            ],
            "Resource": "arn:aws:iam::123456789012:role/aws-service-role/
guardduty.amazonaws.com/AWSServiceRoleForAmazonGuardDuty"
        }
    ]
}
```

Usando uma política personalizada do IAM para limitar o acesso aos GuardDuty recursos

Para definir o acesso de um usuário GuardDuty com base no ID do detector, você pode usar todas as ações de GuardDuty API em suas políticas personalizadas do IAM, exceto as seguintes operações:

- `guardduty:CreateDetector`
- `guardduty:DeclineInvitations`
- `guardduty:DeleteInvitations`
- `guardduty:GetInvitationsCount`
- `guardduty:ListDetectors`
- `guardduty:ListInvitations`

Use as seguintes operações em uma política do IAM para definir o acesso de um usuário GuardDuty com base no ID e no ID do IPset ThreatIntelSet :

- `guardduty:DeleteIPSet`
- `guardduty:DeleteThreatIntelSet`
- `guardduty:GetIPSet`
- `guardduty:GetThreatIntelSet`
- `guardduty:UpdateIPSet`

- `guardduty:UpdateThreatIntelSet`

Os exemplos a seguir mostram como criar políticas usando algumas das operações anteriores:

- Esta política permite que um usuário execute a operação `guardduty:UpdateDetector` usando o ID do detector de 1234567 na região us-east-1:

  JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "guardduty:UpdateDetector"
            ],
            "Resource": "arn:aws:guardduty:us-
east-1:123456789012:detector/1234567"
        }
    ]
}
```

- Esta política permite que um usuário execute a operação `guardduty:UpdateIPSet` usando o ID do detector de 1234567 e o ID de IPSet de 000000 na região us-east-1:

> **Note**
>
> Certifique-se de que o usuário tenha as permissões necessárias para acessar listas de IP confiáveis e listas de ameaças em GuardDuty. Para obter mais informações, consulte Configuração de pré-requisitos para listas de entidades e listas de endereços IP.

  JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
```

```
                "guardduty:UpdateIPSet"
            ],
            "Resource": "arn:aws:guardduty:us-
east-1:123456789012:detector/1234567/ipset/000000"
        }
    ]
}
```

- Esta política permite que um usuário execute a operação `guardduty:UpdateIPSet` usando qualquer ID de detector e o ID de IPSet de 000000 na região us-east-1:

> **Note**
>
> Certifique-se de que o usuário tenha as permissões necessárias para acessar listas de IP confiáveis e listas de ameaças em GuardDuty. Para obter mais informações, consulte Configuração de pré-requisitos para listas de entidades e listas de endereços IP.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "guardduty:UpdateIPSet"
            ],
            "Resource": "arn:aws:guardduty:us-east-1:123456789012:detector/*/
ipset/000000"
        }
    ]
}
```

- Esta política permite que um usuário execute a operação `guardduty:UpdateIPSet` usando o ID de detector e qualquer ID de IPSet na região us-east-1:

> **Note**
>
> Certifique-se de que o usuário tenha as permissões necessárias para acessar listas de IP confiáveis e listas de ameaças em GuardDuty. Para obter mais informações, consulte Configuração de pré-requisitos para listas de entidades e listas de endereços IP.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "guardduty:UpdateIPSet"
            ],
            "Resource": "arn:aws:guardduty:us-
east-1:123456789012:detector/1234567/ipset/*"
        }
    ]
}
```

O ARN do recurso IAM para uma GuardDuty ação corresponde ao caminho do recurso de API dessa ação. A maioria das ações é mapeada para o detector ou um sub-recurso. Por exemplo`detector/detectorId`, `guardduty:GetDetector` usos e `guardduty:GetFilter` usos`detector/detectorId/filter/filterName`.

A maioria das descobertas e ações dos membros acrescentam o nome da operação como um sufixo no caminho do recurso. As operações de lista são a exceção: `guardduty:ListFindings` e `guardduty:ListMembers` usam a base `findings` e `member` os caminhos sem sufixo. Inclua o caminho completo ao definir o escopo de uma política para estas ações:

- `guardduty:GetFindings`usa `detector/detectorId/findings/get`
- `guardduty:GetFindingsStatisticsusa` `detector/detectorId/findings/statistics`
- `guardduty:ArchiveFindingsusa` `detector/detectorId/findings/archive`
- `guardduty:GetMembersusa` `detector/detectorId/member/get`

- `guardduty:ListFindings`usos `detector/detectorId/findings` (sem sufixo)
- `guardduty:ListMembers`usos `detector/detectorId/member` (sem sufixo)

A política a seguir `guardduty:GetFindings` concede um detector específico na região us-east-1, usando o caminho completo do recurso:

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": "guardduty:GetFindings",
    "Resource": "arn:aws:guardduty:us-
east-1:111122223333:detector/a1b2c3d4e5f6g7h8i9j0k1l2m3n4o5p6/findings/get"
  }]
}
```

Usando funções vinculadas a serviços para a Amazon GuardDuty

A Amazon GuardDuty usa funções vinculadas a serviços AWS Identity and Access Management (IAM). Uma função vinculada a serviços (SLR) é um tipo exclusivo de função do IAM diretamente vinculada. GuardDuty Service-linked as funções são predefinidas GuardDuty e incluem todas as permissões GuardDuty necessárias para chamar outros AWS serviços em seu nome.

Com a função vinculada ao serviço, você pode configurar GuardDuty sem adicionar manualmente as permissões necessárias. GuardDuty define as permissões de sua função vinculada ao serviço e, a menos que as permissões sejam definidas de outra forma, somente GuardDuty pode assumir a função. As permissões definidas incluem a política de confiança e a política de permissões, e essa política de permissões não pode ser anexada a nenhuma outra entidade do IAM.

GuardDuty suporta o uso de funções vinculadas a serviços em todas as regiões onde GuardDuty está disponível. Para obter mais informações, consulte Regiões e endpoints.

Você pode excluir a função GuardDuty vinculada ao serviço somente após a primeira desativação GuardDuty em todas as regiões em que ela está ativada. Isso protege seus GuardDuty recursos porque você não pode remover inadvertidamente a permissão para acessá-los.

Para obter informações sobre outros serviços que oferecem suporte a funções vinculadas a serviços, consulte AWS os serviços que funcionam com o IAM no Guia do usuário do IAM e procure os serviços que têm Sim na coluna Service-Linked Função. Escolha um Sim com um link para visualizar a documentação do perfil vinculado para esse serviço.

Service-linked permissões de função para GuardDuty

GuardDuty usa a função vinculada ao serviço (SLR) chamada. `AWSServiceRoleForAmazonGuardDuty` A SLR permite GuardDuty realizar as seguintes tarefas. Também GuardDuty permite incluir os metadados recuperados pertencentes à instância do EC2 nas descobertas que GuardDuty podem gerar sobre a ameaça em potencial. O perfil vinculado ao serviço `AWSServiceRoleForAmazonGuardDuty` confia no serviço `guardduty.amazonaws.com` para presumir o perfil.

As políticas de permissão ajudam a GuardDuty realizar as seguintes tarefas:

- Use as ações do Amazon EC2 para gerenciar e recuperar informações sobre suas instâncias, imagens e componentes de rede do EC2, como VPCs, sub-redes, gateways.
- Use AWS Systems Manager ações para gerenciar associações de SSM em instâncias do Amazon EC2 ao ativar o monitoramento de GuardDuty tempo de execução com um agente automatizado para o Amazon EC2. Quando a configuração GuardDuty automatizada do agente está desativada, GuardDuty considera somente as instâncias do EC2 que têm uma tag de inclusão (`GuardDutyManaged:true`).
- Use AWS Organizations ações para descrever contas associadas e ID da organização.
- Use as ações do Amazon S3 para recuperar informações sobre buckets e objetos do S3.
- Use AWS Lambda ações para recuperar informações sobre suas funções e tags do Lambda.
- Use as ações do Amazon EKS para gerenciar e recuperar informações sobre os clusters do EKS e gerenciar os complementos do Amazon EKS nos clusters do EKS. As ações do EKS também recuperam as informações sobre as tags associadas a. GuardDuty
- Use o IAM para criar o Service-linked permissões de função para proteção contra malware para EC2 após a habilitação da Proteção contra malware para EC2.
- Use as ações do Amazon ECS para gerenciar e recuperar informações sobre os clusters do Amazon ECS, recuperar informações sobre tarefas e definições de tarefas e gerenciar a configuração da conta do Amazon ECS com. `guarddutyActivate` As ações relacionadas ao Amazon ECS também recuperam as informações sobre as tags associadas a. GuardDuty
- Use as ações do Amazon VPC Lattice para habilitar a conectividade para o agente de monitoramento de tempo de execução.

A função é configurada com a seguinte política gerenciada da AWS, denominada `AmazonGuardDutyServiceRolePolicy`.

Para verificar as permissões para esta política, consulte AmazonGuardDutyServiceRolePolicy no Guia de referência de políticas gerenciadas pela AWS .

Veja a seguir a política de confiança anexada à função vinculada a serviço `AWSServiceRoleForAmazonGuardDuty`:

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "guardduty.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Para obter detalhes sobre atualizações da política do `AmazonGuardDutyServiceRolePolicy`, consulte GuardDuty atualizações para AWS políticas gerenciadas. Para obter alertas automáticos sobre alterações feitas nesta política, inscreva-se no feed RSS na página Histórico do documento.

Criação de uma função vinculada ao serviço para GuardDuty

A função `AWSServiceRoleForAmazonGuardDuty` vinculada ao serviço é criada automaticamente quando você a ativa GuardDuty pela primeira vez ou habilita GuardDuty em uma região com suporte na qual você não a habilitava anteriormente. Você também pode criar a função vinculada ao serviço manualmente usando o console do IAM AWS CLI, a ou a API do IAM.

> **Important**
>
> A função vinculada ao serviço criada para a conta GuardDuty delegada do administrador não se aplica às contas dos membros. GuardDuty

É necessário configurar permissões para que uma entidade do IAM (por exemplo, um usuário, grupo ou função) crie, edite ou exclua uma função vinculada ao serviço. Para que a função `AWSServiceRoleForAmazonGuardDuty` vinculada ao serviço seja criada com sucesso, o principal do IAM que você usa GuardDuty deve ter as permissões necessárias. Para conceder as permissões necessárias, anexe a seguinte política ao usuário, grupo ou função do :

> **Note**
>
> Substitua a amostra *`account ID`* no exemplo a seguir pela sua Conta da AWS ID real.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "guardduty:*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:CreateServiceLinkedRole"
            ],
            "Resource": "arn:aws:iam::123456789012:role/aws-service-role/
guardduty.amazonaws.com/AWSServiceRoleForAmazonGuardDuty",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "guardduty.amazonaws.com"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:PutRolePolicy",
                "iam:DeleteRolePolicy"
```

```
            ],
            "Resource": "arn:aws:iam::123456789012:role/aws-service-role/
guardduty.amazonaws.com/AWSServiceRoleForAmazonGuardDuty"
        }
    ]
}
```

Para mais informações sobre a criação da função manualmente, consulte Criar uma função vinculada ao serviço no Guia do usuário do IAM.

Editando uma função vinculada ao serviço para GuardDuty

GuardDuty não permite que você edite a função `AWSServiceRoleForAmazonGuardDuty` vinculada ao serviço. Depois que você criar um perfil vinculado ao serviço, não poderá alterar o nome do perfil, pois várias entidades podem fazer referência ao perfil. No entanto, você poderá editar a descrição do perfil usando o IAM. Para saber mais, consulte Editar um perfil vinculado ao serviço no Guia do usuário do IAM.

Excluindo uma função vinculada ao serviço para GuardDuty

Se você não precisar mais usar um atributo ou serviço que requer um perfil vinculado ao serviço, é recomendável excluí-lo. Dessa forma, você não terá uma entidade não utilizada que não seja monitorada ativamente ou mantida.

> **Important**
>
> Se você habilitou a Proteção contra malware para EC2, a exclusão `AWSServiceRoleForAmazonGuardDuty` não exclui `AWSServiceRoleForAmazonGuardDutyMalwareProtection` automaticamente. Se você deseja excluir `AWSServiceRoleForAmazonGuardDutyMalwareProtection`, consulte Excluir uma função vinculada ao serviço para a Proteção contra malware para EC2.

Você deve primeiro desabilitar GuardDuty em todas as regiões em que ele está ativado para excluir `AWSServiceRoleForAmazonGuardDuty` o. Se o GuardDuty serviço não estiver desativado quando você tentar excluir a função vinculada ao serviço, a exclusão falhará. Para obter mais informações, consulte Suspensão ou desativação GuardDuty.

Quando você desativa GuardDuty, o `AWSServiceRoleForAmazonGuardDuty` não é excluído automaticamente. Se você ativar GuardDuty novamente, ele começará a usar o existente`AWSServiceRoleForAmazonGuardDuty`.

Como excluir manualmente o perfil vinculado ao serviço usando o IAM

Use o console do IAM AWS CLI, a ou a API do IAM para excluir a função `AWSServiceRoleForAmazonGuardDuty` vinculada ao serviço. Para saber mais, consulte Excluir um perfil vinculado ao serviço no Guia do usuário do IAM.

Compatível Regiões da AWS

A Amazon GuardDuty suporta o uso da função `AWSServiceRoleForAmazonGuardDuty` vinculada ao serviço em todos os Regiões da AWS lugares disponíveis GuardDuty . Para obter uma lista das regiões em que GuardDuty está disponível atualmente, consulte GuardDuty Endpoints e cotas da Amazon no. Referência geral da Amazon Web Services

Service-linked permissões de função para proteção contra malware para EC2

A Proteção contra malware para EC2 usa a função vinculada ao serviço (SLR) chamada `AWSServiceRoleForAmazonGuardDutyMalwareProtection`. Essa SLR permite que o Malware Protection for EC2 realize escaneamentos sem agente para detectar malware em sua conta. GuardDuty Ele permite GuardDuty criar um instantâneo de volume do EBS em sua conta e compartilhar esse instantâneo com a GuardDuty conta de serviço. Depois de GuardDuty avaliar o snapshot, ele inclui os metadados da carga de trabalho da instância e do contêiner do EC2 recuperados nas descobertas do Malware Protection for EC2. O perfil vinculado ao serviço `AWSServiceRoleForAmazonGuardDutyMalwareProtection` confia no serviço `malware-protection.guardduty.amazonaws.com` para presumir o perfil.

As políticas de permissão para essa função ajudam a Proteção contra malware para EC2 a realizar as seguintes tarefas:

- Use ações do Amazon Elastic Compute Cloud (Amazon EC2) para recuperar informações sobre instâncias, volumes e snapshots do Amazon EC2. A Proteção contra malware para EC2 também fornece permissão para acessar os metadados de cluster do Amazon EKS e do Amazon ECS.
- Crie snapshots para volumes do EBS que tenham a tag `GuardDutyExcluded` não definida como `true`. Por padrão, os snapshots são criados com uma tag `GuardDutyScanId`. Não remova essa tag, caso contrário, a Proteção contra malware para EC2 não terá acesso aos snapshots.

> **Important**
>
> Quando você define como`true`, o GuardDuty serviço não poderá acessar esses instantâneos no futuro. `GuardDutyExcluded` Isso ocorre porque as outras instruções nessa função vinculada ao serviço GuardDuty impedem a execução de qualquer ação nos instantâneos que tenham o `GuardDutyExcluded` definido como. `true`

- Permita o compartilhamento e a exclusão de snapshots somente se a tag `GuardDutyScanId` existir e a tag `GuardDutyExcluded` não estiver definida como `true`.

> **Note**
>
> Não permite que a Proteção contra malware para EC2 torne os snapshots públicos.

- Acesse as chaves gerenciadas pelo cliente, exceto aquelas que têm uma `GuardDutyExcluded` tag definida como`true`, para ligar `CreateGrant` para criar e acessar um volume EBS criptografado a partir do snapshot criptografado que é compartilhado com a conta de GuardDuty serviço. Para obter uma lista de contas de GuardDuty serviço para cada região, consulte[GuardDuty contas de serviço por Região da AWS](#).
- Acesse CloudWatch os registros dos clientes para criar o grupo de registros do Malware Protection for EC2, bem como colocar os registros de eventos de verificação de malware no `/aws/guardduty/malware-scan-events` grupo de registros.
- Permita que o cliente decida se deseja manter os snapshots nos quais o malware foi detectado em sua conta. Se o escaneamento detectar malware, a função vinculada ao serviço permitirá adicionar duas tags GuardDuty aos instantâneos - e. `GuardDutyFindingDetected` `GuardDutyExcluded`

> **Note**
>
> A tag `GuardDutyFindingDetected` especifica que os snapshots contêm malware.

- Determine se um volume está criptografado com uma chave gerenciada pelo EBS. GuardDuty executa a `DescribeKey` ação para determinar `key Id` a EBS-managed chave em sua conta.
- Obtenha o instantâneo dos volumes do EBS criptografados usando Chave gerenciada pela AWS, do seu Conta da AWS e copie-o para o. [GuardDuty conta de serviço](#) Para isso, usamos as permissões `GetSnapshotBlock` `ListSnapshotBlocks` e. GuardDuty em seguida, digitalizará

o instantâneo na conta de serviço. Atualmente, o suporte do Malware Protection for EC2 para escanear volumes do EBS criptografados com Chave gerenciada pela AWS pode não estar disponível em todos os. Regiões da AWS Para obter mais informações, consulte Region-specific disponibilidade de recursos.

- Permita que o Amazon EC2 ligue AWS KMS em nome do Malware Protection for EC2 para realizar várias ações criptográficas nas chaves gerenciadas pelo cliente. Ações como `kms:ReEncryptTo` e `kms:ReEncryptFrom` são necessárias para compartilhar os snapshots criptografados com as chaves gerenciadas pelo cliente. Somente as chaves para as quais a tag `GuardDutyExcluded` não está definida como `true` estão acessíveis.

A função é configurada com a seguinte política gerenciada da AWS, denominada `AmazonGuardDutyMalwareProtectionServiceRolePolicy`.

Para verificar as permissões para esta política, consulte AmazonGuardDutyMalwareProtectionServiceRolePolicy no Guia de referência de políticas gerenciadas pela AWS .

A seguinte política de confiança está anexada à função vinculada a serviço `AWSServiceRoleForAmazonGuardDutyMalwareProtection`:

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "malware-protection.guardduty.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Criar uma função vinculada ao serviço para Proteção contra malware para EC2

A função vinculada ao serviço `AWSServiceRoleForAmazonGuardDutyMalwareProtection` é criada automaticamente quando você habilita a Proteção contra Malware para EC2 pela primeira vez ou habilita a Proteção contra Malware para EC2 em uma região com suporte em que ela não tenha sido habilitada anteriormente. Também é possível criar a função vinculada ao serviço `AWSServiceRoleForAmazonGuardDutyMalwareProtection` manualmente usando o console do IAM, o IAM CLI ou o IAM API.

> **Note**
>
> Por padrão, se você for novo na Amazon GuardDuty, a Proteção contra Malware para EC2 é ativada automaticamente.

> **Important**
>
> A função vinculada ao serviço criada para a conta delegada do GuardDuty administrador não se aplica às contas dos membros. GuardDuty

É necessário configurar permissões para que uma entidade do IAM (por exemplo, um usuário, grupo ou função) crie, edite ou exclua uma função vinculada ao serviço. Para que a função `AWSServiceRoleForAmazonGuardDutyMalwareProtection` vinculada ao serviço seja criada com sucesso, a identidade do IAM que você usa GuardDuty deve ter as permissões necessárias. Para conceder as permissões necessárias, anexe a seguinte política ao usuário, grupo ou função do :

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": "guardduty:*",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
```

```
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": [
                        "malware-protection.guardduty.amazonaws.com"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "organizations:EnableAWSServiceAccess",
                "organizations:RegisterDelegatedAdministrator",
                "organizations:ListDelegatedAdministrators",
                "organizations:ListAWSServiceAccessForOrganization",
                "organizations:DescribeOrganizationalUnit",
                "organizations:DescribeAccount",
                "organizations:DescribeOrganization"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:GetRole",
            "Resource": "arn:aws:iam::*:role/
*AWSServiceRoleForAmazonGuardDutyMalwareProtection"
        }
    ]
}
```

Para obter mais informações sobre como criar a função manualmente, consulte Criar uma função vinculada ao serviço no Guia do usuário do IAM.

Editar uma função vinculada ao serviço para Proteção contra malware para EC2

A Proteção contra Malware para EC2 não permite que você edite a função vinculada a serviço `AWSServiceRoleForAmazonGuardDutyMalwareProtection`. Depois que você criar um perfil vinculado ao serviço, não poderá alterar o nome do perfil, pois várias entidades podem fazer referência ao perfil. No entanto, você poderá editar a descrição do perfil usando o IAM. Para saber mais, consulte Editar um perfil vinculado ao serviço no Guia do usuário do IAM.

Excluir uma função vinculada ao serviço para a Proteção contra malware para EC2

Se você não precisar mais usar um atributo ou serviço que requer um perfil vinculado ao serviço, é recomendável excluí-lo. Dessa forma, você não terá uma entidade não utilizada que não seja monitorada ativamente ou mantida.

> **Important**
>
> Você deverá primeiramente desabilitar a Proteção contra Malware para EC2 em todas as regiões em que estiver habilitada para excluir o `AWSServiceRoleForAmazonGuardDutyMalwareProtection`.
> Se a Proteção contra malware para EC2 não estiver desabilitada quando você tentar excluir a função vinculada ao serviço, haverá falha na exclusão. Lembre-se de desabilitar primeiro a Proteção contra malware para o EC2 em sua conta.

Quando você escolhe Desabilitar para interromper o serviço de Proteção contra malware para EC2, o não `AWSServiceRoleForAmazonGuardDutyMalwareProtection` é excluído automaticamente. Se você escolher Habilitar para iniciar o serviço Malware Protection for EC2 novamente, GuardDuty começará a usar o existente`AWSServiceRoleForAmazonGuardDutyMalwareProtection`.

Como excluir manualmente o perfil vinculado ao serviço usando o IAM

Use o console do IAM, a AWS CLI ou a API do IAM para excluir a função vinculada ao `AWSServiceRoleForAmazonGuardDutyMalwareProtection` serviço. Para saber mais, consulte Excluir um perfil vinculado ao serviço no Guia do usuário do IAM.

Compatível Regiões da AWS

A Amazon GuardDuty suporta o uso da função `AWSServiceRoleForAmazonGuardDutyMalwareProtection` vinculada ao serviço em todos os Regiões da AWS lugares em que o Malware Protection for EC2 está disponível.

Para obter uma lista das regiões em que GuardDuty está disponível atualmente, consulte GuardDuty Endpoints e cotas da Amazon no. Referência geral da Amazon Web Services

AWS políticas gerenciadas para a Amazon GuardDuty

Para adicionar permissões a usuários, grupos e funções, é mais fácil usar políticas AWS gerenciadas do que criar políticas você mesmo. É necessário tempo e experiência para criar políticas gerenciadas

pelo cliente do IAM que fornecem à sua equipe apenas as permissões de que precisam. Para começar rapidamente, você pode usar nossas políticas AWS gerenciadas. Essas políticas abrangem casos de uso comuns e estão disponíveis na sua Conta da AWS. Para obter mais informações sobre políticas AWS gerenciadas, consulte políticas AWS gerenciadas no Guia do usuário do IAM.

AWS os serviços mantêm e atualizam as políticas AWS gerenciadas. Você não pode alterar as permissões nas políticas AWS gerenciadas. Ocasionalmente, os serviços adicionam permissões adicionais a uma política AWS gerenciada para oferecer suporte a novos recursos. Esse tipo de atualização afeta todas as identidades (usuários, grupos e funções) em que a política está anexada. É mais provável que os serviços atualizem uma política AWS gerenciada quando um novo recurso é lançado ou quando novas operações são disponibilizadas. Os serviços não removem as permissões de uma política AWS gerenciada, portanto, as atualizações da política não quebrarão suas permissões existentes.

Além disso, AWS oferece suporte a políticas gerenciadas para funções de trabalho que abrangem vários serviços. Por exemplo, a política ReadOnlyAccess AWS gerenciada fornece acesso somente para leitura a todos os AWS serviços e recursos. Quando um serviço lança um novo recurso, AWS adiciona permissões somente de leitura para novas operações e recursos. Para obter uma lista e descrições das políticas de perfis de trabalho, consulte Políticas gerenciadas pela AWS para perfis de trabalho no Guia do usuário do IAM.

O elemento de política `Version` especifica as regras de sintaxe de linguagem que devem ser usadas para processar uma política. As políticas a seguir incluem a versão atual compatível com o IAM. Para obter mais informações, consulte Elementos da política JSON do IAM: Versão.

AWS política gerenciada: AmazonGuardDutyFullAccess_v2 (recomendado)

É possível anexar a política AmazonGuardDutyFullAccess_v2 às suas identidades do IAM. Essa política permitirá que o usuário tenha acesso total para realizar todas as GuardDuty ações e acessar os recursos necessários. Between AmazonGuardDutyFullAccess_v2 e AmazonGuardDutyFullAccess, GuardDuty recomenda a anexação AmazonGuardDutyFullAccess_v2 porque oferece maior segurança e restringe as ações administrativas aos diretores de GuardDuty serviços.

Detalhes de permissões

A política AmazonGuardDutyFullAccess_v2 inclui as seguintes permissões:

- `GuardDuty`— Permite que os usuários tenham acesso total a todas GuardDuty as ações.
- `IAM`:
  - Permite que os usuários criem funções GuardDuty vinculadas ao serviço.
  - Permite visualizar e gerenciar funções do IAM e suas políticas para GuardDuty.
  - Permite que os usuários passem uma função para GuardDuty o. GuardDuty usa essa função para ativar a proteção contra malware para o S3 e escanear objetos do S3 em busca de malware. GuardDuty também usa essa função para iniciar escaneamentos de proteção contra malware para backup. AWS
  - A permissão para realizar uma ação `iam:GetRole` no `AWSServiceRoleForAmazonGuardDutyMalwareProtection` estabelece se o perfil vinculado ao serviço (SLR) da Proteção contra malware existe em uma conta.
- `Organizations`:
  - Permita que os usuários leiam (visualizem) a estrutura e as contas da GuardDuty organização.
  - Permite que os usuários designem um administrador delegado e gerenciem membros de uma GuardDuty organização.

Para revisar as permissões dessa política, consulte AmazonGuardDutyFullAccess _v2 no Guia de referência de políticas AWS gerenciadas.

AWS política gerenciada: AmazonGuardDutyFullAccess

É possível anexar a política `AmazonGuardDutyFullAccess` às suas identidades do IAM.

> **Important**
>
> Para maior segurança e permissões restritivas aos diretores GuardDuty de serviços, recomendamos que você use. AWS política gerenciada: AmazonGuardDutyFullAccess_v2 (recomendado)

Essa política concede permissões administrativas que permitem ao usuário acesso total para realizar todas as GuardDuty ações e recursos.

Detalhes da permissão

Esta política inclui as seguintes permissões.

- `GuardDuty`— Permite que os usuários tenham acesso total a todas GuardDuty as ações.
- `IAM`:
  - Permite que os usuários criem a função GuardDuty vinculada ao serviço.
  - Permite que uma conta de administrador seja ativada GuardDuty para contas de membros.
  - Permite que os usuários passem uma função para GuardDuty o. GuardDuty usa essa função para ativar a proteção contra malware para o S3 e escanear objetos do S3 em busca de malware. GuardDuty também usa essa função para iniciar escaneamentos de proteção contra malware para backup. AWS
- `Organizations`— Permite que os usuários designem um administrador delegado e gerenciem os membros de uma GuardDuty organização.

A permissão para realizar uma ação `iam:GetRole` no `AWSServiceRoleForAmazonGuardDutyMalwareProtection` estabelece se o perfil vinculado ao serviço (SLR) da Proteção contra malware existe em uma conta.

Para verificar as permissões para esta política, consulte AmazonGuardDutyFullAccess no Guia de referência de políticas gerenciadas pela AWS .

AWS política gerenciada: AmazonGuardDutyReadOnlyAccess

É possível anexar a política `AmazonGuardDutyReadOnlyAccess` às suas identidades do IAM.

Essa política concede permissões somente para leitura que permitem ao usuário visualizar GuardDuty descobertas e detalhes da sua GuardDuty organização.

Detalhes das permissões

Esta política inclui as seguintes permissões.

- `GuardDuty`— Permite que os usuários visualizem GuardDuty as descobertas e realizem operações de API que começam com `GetList`,, ou`Describe`.
- `Organizations`— Permite que os usuários recuperem informações sobre a configuração GuardDuty da sua organização, incluindo detalhes da conta de administrador delegada.

Para verificar as permissões para esta política, consulte AmazonGuardDutyReadOnlyAccess no Guia de referência de políticas gerenciadas pela AWS .

AWS política gerenciada: AmazonGuardDutyServiceRolePolicy

Não é possível anexar a `AmazonGuardDutyServiceRolePolicy` às entidades do IAM. Essa política AWS gerenciada está vinculada a uma função vinculada ao serviço que permite GuardDuty realizar ações em seu nome. Para obter mais informações, consulte Service-linked permissões de função para GuardDuty.

GuardDuty atualizações para AWS políticas gerenciadas

Veja detalhes sobre as atualizações das políticas AWS gerenciadas GuardDuty desde que esse serviço começou a rastrear essas alterações. Para receber alertas automáticos sobre alterações nesta página, assine o feed RSS na página Histórico do GuardDuty documento.

Alteração	Descrição	Data
AmazonGuardDutyServiceRolePolicy: atualizar para uma política existente	Foram adicionadas as `vpc-lattice:AssociateViaAWSService` permissões `vpc-lattice:CreateServiceNetworkVpcAssociation` e, que permitem GuardDuty usar as ações do Amazon VPC Lattice para habilitar a conectividade para o agente de monitoramento de tempo de execução. A `GdLatticeCreateManagedSnvaAssociation` declaração permite GuardDuty criar uma associação VPC de rede de serviços para recursos na mesma conta. A `GdLatticeAssociate`	9 de setembro de 2026

Alteração	Descrição	Data
	`ViaAwsService` declaração permite concluir GuardDuty a associação por meio do Amazon VPC Lattice. `{ "Sid": "GdLatticeCreateManagedSnvaAssociation", "Effect": "Allow", "Action": "vpc-lattice:CreateServiceNetworkVpcAssociation", "Resource": "arn:aws:vpc-lattice:*:*:servicenetworkvpcassociation/*", "Condition": { "StringEquals": { "aws:ResourceAccount": "${aws:PrincipalAccount}" } } }, {`	

Alteração	Descrição	Data
	"Sid": "GdLatticeAssociateViaAwsService", "Effect": "Allow", "Action": "vpc-lattice:AssociateViaAWSService", "Resource": "*" }	
AmazonGuardDutyServiceRolePolicy – atualização para uma política existente	Foi adicionada `s3:ListBucket` permissão para recuperar listagens de buckets do S3 `ecs:DescribeTasks` e `ecs:DescribeTaskDefinition` permissões para recuperar informações sobre tarefas e definições de tarefas do Amazon ECS.	23 de abril de 2026

Alteração	Descrição	Data
AmazonGuardDutyServiceRolePolicy – atualização para uma política existente	Foi adicionada a `cloudtrail:CreateServiceLinkedChannel` permissão para ativar um mecanismo adicional para consumir AWS CloudTrail eventos. `{ "Sid": "CloudTrailCreateServiceLinkedChannelSid", "Effect": "Allow", "Action": [ "cloudtrail:CreateServiceLinkedChannel" ], "Resource": "arn:aws:cloudtrail:*:*:channel/aws-service-channel/guardduty/*", "Condition": { "StringEquals": { "aws:ResourceAccount": "${aws:PrincipalAccount}"`	25 de março de 2026

Alteração	Descrição	Data
	`}` `}` `}`	
`AmazonGuardDutyFullAccess` : descontinuada	Esta política foi substituída por uma política com escopo reduzido chamada `AmazonGuardDutyFullAccess_v2` . Depois de 13 de março de 2026, você não poderá vincular a `AmazonGuardDutyFullAccess` política a novos usuários, grupos ou funções. Para obter mais informações, consulte AWS política gerenciada: AmazonGuardDutyFullAccess_v2 (recomendado).	13 de março de 2026

Alteração	Descrição	Data

AmazonGuardDutyFullAccess_v2 – atualização para uma política existente	Foi adicionada uma permissão que permite passar uma função do IAM para GuardDuty quando você ativa a Proteção contra malware para AWS backup.
	
	{
	
	"Sid": "AllowPassRoleToMalwareProtection",
	
	"Effect": "Allow",
	
	"Action": [
	
	"iam:PassRole"
	
	],
	
	"Resource": "arn:aws:iam::*:role/*",
	
	"Condition": {
	
	"StringEquals": {
	
	"iam:PassedToService": [
	
	"malware-protectio
		19 de novembro de 2025

Alteração	Descrição	Data
	n-plan.guardduty.amazonaws.com", "malware-protection.guardduty.amazonaws.com"] } } }	

Alteração	Descrição	Data

AmazonGuardDutyFullAccess – atualização para uma política existente	Foi adicionada uma permissão que permite passar uma função do IAM para GuardDuty quando você ativa a Proteção contra malware para AWS backup.
	
	{
	
	"Sid": "AllowPassRoleToMalwareProtection",
	
	"Effect": "Allow",
	
	"Action": [
	
	"iam:PassRole"
	
	],
	
	"Resource": "arn:aws:iam::*:role/*",
	
	"Condition": {
	
	"StringEquals": {
	
	"iam:PassedToService": [
	
	"malware-protectio
		19 de novembro de 2025

Alteração	Descrição	Data
	n-plan.guardduty.amazonaws.com", "malware-protection.guardduty.amazonaws.com"] } } }	
AmazonGuardDutyFullAccess_v2 - Adicionou uma nova política	Nova política AmazonGuardDutyFullAccess_v2 adicionada. Isso é recomendado porque suas permissões aumentam a segurança ao restringir as ações administrativas aos diretores GuardDuty de serviço com base nas funções e políticas do IAM e na integração. AWS Organizations	04 de junho de 2025
AmazonGuardDutyServiceRolePolicy – atualização para uma política existente	Adicionou a permissão `ec2:DescribeVpcs` . Isso permite GuardDuty rastrear as atualizações da VPC, como recuperar o CIDR da VPC.	22 de agosto de 2024

Alteração	Descrição	Data

AmazonGuardDutyFullAccess – atualização para uma política existente	Foi adicionada uma permissão que permite passar uma função do IAM para GuardDuty quando você ativa a Proteção contra malware para o S3.
	
	{
	"Sid": "AllowPassRoleToMalwareProtectionPlan",
	"Effect": "Allow",
	"Action": [
	"iam:PassRole"
	],
	"Resource": "arn:aws:iam::*:role/*",
	"Condition": {
	"StringEquals": {
	"iam:PassedToService": "malware-protection-plan.guardduty.amazonaws.com"
	}
	}
	}
		10 de junho de 2024

Alteração	Descrição	Data
AmazonGuardDutyServiceRolePolicy: atualizar para uma política existente.	Use AWS Systems Manager ações para gerenciar associações de SSM em instâncias do Amazon EC2 ao ativar o monitoramento de GuardDuty tempo de execução com um agente automatizado para o Amazon EC2. Quando a configuração GuardDuty automatizada do agente está desativada, GuardDuty considera somente as instâncias do EC2 que têm uma tag de inclusão (`GuardDutyManaged :true`).	26 de março de 2024
AmazonGuardDutyServiceRolePolicy: atualizar para uma política existente.	GuardDuty adicionou uma nova permissão: recuperar `organization:DescribeOrganization` a ID da organização da conta compartilhada da Amazon VPC e definir a política de endpoint da Amazon VPC com a ID da organização.	9 de fevereiro de 2024

Alteração	Descrição	Data
AmazonGuardDutyMalwareProtectionServiceRolePolicy: atualizar para uma política existente.	O Malware Protection for EC2 adicionou duas permissões: `ListSnapshotBlocks` obter o instantâneo de um volume do EBS (criptografado usando Chave gerenciada pela AWS) do seu Conta da AWS e copiá-lo para a conta de GuardDuty serviço antes de iniciar a verificação de malware. `GetSnapshotBlock`	25 de janeiro de 2024
AmazonGuardDutyServiceRolePolicy – atualização para uma política existente	Foram adicionadas novas permissões GuardDuty para permitir adicionar configurações de conta do `guardduty Activate` Amazon ECS e realizar operações de lista e descrição em clusters do Amazon ECS.	26 de novembro de 2023
AmazonGuardDutyReadOnlyAccess – atualização para uma política existente	GuardDuty adicionou uma nova política `organizations` para `ListAccounts`o.	16 de novembro de 2023
AmazonGuardDutyFullAccess – atualização para uma política existente	GuardDuty adicionou uma nova política `organizations` para `ListAccounts`o.	16 de novembro de 2023

Alteração	Descrição	Data
AmazonGuardDutyServiceRolePolicy – atualização para uma política existente	GuardDuty adicionou novas permissões para oferecer suporte ao próximo recurso de monitoramento de tempo de execução do GuardDuty EKS.	8 de março de 2023
AmazonGuardDutyServiceRolePolicy – atualização para uma política existente	GuardDuty adicionou novas permissões para permitir GuardDuty a criação de uma Service-linked função de proteção contra malware para EC2. Isso ajudará a GuardDuty simplificar o processo de habilitação da proteção contra malware para o EC2. GuardDuty agora pode realizar a seguinte ação do IAM: `{ "Effect": "Allow", "Action": "iam:CreateServiceLinkedRole", "Resource": "*", "Condition": { "StringEquals": { "iam:AWSServiceName": "malware-protection.guardduty.amazonaws.com" } } }`	21 de fevereiro de 2023

Alteração	Descrição	Data
AmazonGuardDutyFullAccess – atualização para uma política existente	GuardDuty ARN atualizad o `iam:GetRole` para o. `*AWSServiceRoleFor AmazonGuardDutyMal wareProtection`	26 de julho de 2022
AmazonGuardDutyFullAccess: atualização para uma política existente	GuardDuty adicionou uma nova `AWSServiceName` para permitir a criação de uma função vinculada ao serviço usando o `iam:Creat eServiceLinkedRole` serviço GuardDuty Malware Protection for EC2. GuardDuty agora pode realizar a `iam:GetRole` ação para obter informações para`AWSServiceRole` .	26 de julho de 2022

Alteração	Descrição	Data
AmazonGuardDutyServiceRolePolicy: atualização para uma política existente	GuardDuty adicionou novas permissões GuardDuty para permitir o uso de ações de rede do Amazon EC2 para melhorar as descobertas. GuardDuty agora pode realizar as seguintes ações do EC2 para obter informações sobre como suas instâncias do EC2 estão se comunicando. Essas informações são usadas para melhorar a precisão da descoberta. • `ec2:DescribeVpcEndpoints` • `ec2:DescribeSubnets` • `ec2:DescribeVpcPeeringConnections` • `ec2:DescribeTransitGatewayAttachments`	3 de agosto de 2021
GuardDuty começou a rastrear alterações	GuardDuty começou a rastrear mudanças em suas políticas AWS gerenciadas.	3 de agosto de 2021

Solução de problemas de GuardDuty identidade e acesso da Amazon

Use as informações a seguir para ajudá-lo a diagnosticar e corrigir problemas comuns que você pode encontrar ao trabalhar com GuardDuty um IAM.

Tópicos

- Não estou autorizado a realizar uma ação em GuardDuty
- Não estou autorizado a realizar iam:PassRole.
- Quero permitir que pessoas fora da minha Conta da AWS para acessar meus GuardDuty recursos.

Não estou autorizado a realizar uma ação em GuardDuty

Se você receber uma mensagem de erro informando que não tem autorização para executar uma ação, suas políticas deverão ser atualizadas para permitir que você realize a ação.

O erro do exemplo a seguir ocorre quando o usuário do IAM `mateojackson` tenta usar o console para visualizar detalhes sobre um atributo *`my-example-widget`* fictício, mas não tem as permissões `guardduty:`*`GetWidget`* fictícias.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 guardduty:GetWidget on resource: my-example-widget
```

Nesse caso, a política do usuário `mateojackson` deve ser atualizada para permitir o acesso ao recurso *`my-example-widget`* usando a ação `guardduty:`*`GetWidget`*.

Se precisar de ajuda, entre em contato com seu AWS administrador. Seu administrador é a pessoa que forneceu suas credenciais de login.

Não estou autorizado a realizar iam:PassRole.

Se você receber uma mensagem de erro informando que não está autorizado a executar a ação `iam:PassRole`, as suas políticas devem ser atualizadas para permitir que você passe uma função para o GuardDuty.

Alguns Serviços da AWS permitem que você passe uma função existente para esse serviço em vez de criar uma nova função de serviço ou uma função vinculada ao serviço. Para fazê-lo, você deve ter permissões para passar o perfil para o serviço.

O exemplo de erro a seguir ocorre quando uma usuária do IAM chamada `marymajor` tenta utilizar o console para executar uma ação no GuardDuty. No entanto, a ação exige que o serviço tenha permissões concedidas por um perfil de serviço. Mary não tem permissões para passar o perfil para o serviço.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

Nesse caso, as políticas de Mary devem ser atualizadas para permitir que ela realize a ação `iam:PassRole`.

Se precisar de ajuda, entre em contato com seu AWS administrador. Seu administrador é a pessoa que forneceu suas credenciais de login.

Quero permitir que pessoas fora da minha Conta da AWS para acessar meus GuardDuty recursos.

É possível criar um perfil que os usuários de outras contas ou pessoas fora da organização podem usar para acessar seus recursos. É possível especificar quem é confiável para assumir o perfil. Para serviços que oferecem compatibilidade com políticas baseadas em recursos ou listas de controle de acesso (ACLs), é possível usar essas políticas para conceder às pessoas acesso aos seus recursos.

Para saber mais, consulte:

- Para saber se é GuardDuty compatível com esses recursos, consulteComo a Amazon GuardDuty trabalha com o IAM.
- Para saber como fornecer acesso aos seus recursos em todos os Contas da AWS que você possui, consulte Como fornecer acesso a um usuário do IAM em outro Conta da AWS que você possui no Guia do usuário do IAM.
- Para saber como fornecer acesso aos seus recursos a terceiros Contas da AWS, consulte Como fornecer acesso Contas da AWS a terceiros no Guia do usuário do IAM.
- Para saber como conceder acesso por meio da federação de identidades, consulte Conceder acesso a usuários autenticados externamente (federação de identidades) no Guia do usuário do IAM.
- Para conhecer a diferença entre perfis e políticas baseadas em recurso para acesso entre contas, consulte Acesso a recursos entre contas no IAM no Guia do usuário do IAM.

Validação de conformidade para a Amazon GuardDuty

Nossa nova experiência AWS de inscrição não foi projetada para cargas de trabalho regulamentadas. Se você estiver usando nossa nova experiência de AWS inscrição, mas quiser usá-la AWS para cargas de trabalho regulamentadas, você pode se inscrever AWS (avançado) ou ativar recursos avançados para seu AWS ambiente.

Para saber se um AWS service (Serviço da AWS) está dentro do escopo de programas de conformidade específicos, consulte Serviços da AWS Escopo por Programa de Conformidade e

escolha o programa de conformidade no qual você está interessado. Para obter informações gerais, consulte Programas de AWS conformidade Programas .

Você pode baixar relatórios de auditoria de terceiros usando AWS Artifact. Para obter mais informações, consulte Baixando relatórios em AWS Artifact .

Sua responsabilidade de conformidade durante o uso Serviços da AWS é determinada pela confidencialidade de seus dados, pelos objetivos de conformidade da sua empresa e pelas leis e regulamentações aplicáveis. Para obter mais informações sobre sua responsabilidade de conformidade ao usar Serviços da AWS, consulte a Documentação AWS de segurança.

Resiliência na Amazon GuardDuty

A infraestrutura AWS global é construída em torno de AWS regiões e zonas de disponibilidade. As regiões fornecem várias zonas de disponibilidade separadas e isoladas fisicamente, que são conectadas com baixa latência, alta throughput e redes altamente redundantes. Com as zonas de disponibilidade, é possível projetar e operar aplicações e bancos de dados que automaticamente executam o failover entre as zonas sem interrupção. As zonas de disponibilidade são altamente disponíveis, tolerantes a falhas e escaláveis que uma ou várias infraestruturas de data center tradicionais.

Para obter mais informações sobre AWS regiões e zonas de disponibilidade, consulte infraestrutura AWS global.

Segurança da infraestrutura na Amazon GuardDuty

Como um serviço gerenciado, a Amazon GuardDuty é protegida pela segurança de rede AWS global. Para obter informações sobre serviços AWS de segurança e como AWS proteger a infraestrutura, consulte AWS Cloud Security. Para projetar seu AWS ambiente usando as melhores práticas de segurança de infraestrutura, consulte Proteção de infraestrutura no Security Pillar AWS Well-Architected Framework.

Você usa chamadas de API AWS publicadas para acessar GuardDuty pela rede. Os clientes devem oferecer compatibilidade com:

- Transport Layer Security (TLS). Exigimos TLS 1.2 e recomendamos TLS 1.3.
- Suítes de criptografia com sigilo direto perfeito (PFS), como DHE (Ephemeral) ou ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Diffie-Hellman A maioria dos sistemas modernos, como Java 7 e versões posteriores, comporta esses modos.

Amazon GuardDuty e endpoints VPC de interface ()AWS PrivateLink

Você pode estabelecer uma conexão privada entre sua VPC e a Amazon GuardDuty criando uma interface VPC endpoint. Os endpoints de interface são alimentados por AWS PrivateLinkuma tecnologia que permite acessar GuardDuty APIs de forma privada sem um gateway de internet, dispositivo NAT, conexão VPN ou conexão Direct AWS Connect. As instâncias na sua VPC não precisam de endereços IP públicos para se comunicar com GuardDuty as APIs. O tráfego entre sua VPC e GuardDuty não sai da rede Amazon.

Cada endpoint de interface é representado por uma ou mais Interfaces de Rede Elástica nas sub-redes.

Para mais informações, consulte Endpoints da VPC de interface(AWS PrivateLink) no Guia AWS PrivateLink .

Considerações sobre GuardDuty VPC endpoints

Antes de configurar uma interface para o VPC endpoint GuardDuty, certifique-se de revisar as propriedades e limitações do endpoint da interface no Guia.AWS PrivateLink

GuardDuty suporta fazer chamadas para todas as suas ações de API a partir de sua VPC.

Criação de uma interface VPC endpoint para GuardDuty

Você pode criar um VPC endpoint para o GuardDuty serviço usando o console Amazon VPC ou o (). AWS Command Line Interface AWS CLI Para obter mais informações, consulte Criar um endpoint de interface no Guia do usuário do AWS PrivateLink .

Crie um VPC endpoint para GuardDuty usar o seguinte nome de serviço:

- com.amazonaws. *region*.dever de guarda
- com.amazonaws. *region*.guardduty-fips (endpoint FIPS)

Se você habilitar o DNS privado para o endpoint, poderá fazer solicitações de API GuardDuty usando seu nome DNS padrão para a região, por exemplo,. `guardduty.us-east-1.amazonaws.com`

Para mais informações, consulte Acessar um serviço por meio de um endpoint de interface no Guia do AWS PrivateLink .

Criação de uma política de VPC endpoint para GuardDuty

É possível anexar uma política de endpoint ao endpoint da VPC que controla o acesso ao GuardDuty. Essa política especifica as seguintes informações:

- A entidade principal que pode realizar ações.
- As ações que podem ser realizadas.
- Os recursos aos quais as ações podem ser aplicadas.

Para mais informações, consulte Controlar o acesso a serviços com endpoints da VPC no Guia AWS PrivateLink .

Exemplo: política de VPC endpoint para ações GuardDuty

Veja a seguir um exemplo de uma política de endpoint para GuardDuty. Quando anexada a um endpoint, essa política concede acesso às GuardDuty ações listadas para todos os diretores em todos os recursos.

```
{
   "Statement":[
      {
         "Principal":"*",
         "Effect":"Allow",
         "Action":[
            "guardduty:listDetectors",
            "guardduty:getDetector",
            "guardduty:getFindings"
         ],
         "Resource":"*"
      }
   ]
}
```

Sub-redes compartilhadas

Você não pode criar, descrever, modificar ou excluir endpoints da VPC em sub-redes que são compartilhadas com você. No entanto, é possível usar os endpoints da VPC em sub-redes que são compartilhadas com você. Para obter informações sobre o compartilhamento da VPC, consulte Compartilhar sua VPC com outras contas no Guia do usuário da Amazon VPC.

GuardDuty integração com serviços AWS de segurança

GuardDuty pode ser integrado a outros serviços AWS de segurança. Esses serviços podem ingerir dados GuardDuty para permitir que você visualize as descobertas de novas maneiras. Analise as opções de integração a seguir para saber mais sobre como esse serviço está configurado para funcionar GuardDuty.

Integrando com GuardDuty AWS Security Hub CSPM

AWS Security Hub CSPM coleta dados de segurança de suas AWS contas, serviços e produtos de parceiros terceirizados compatíveis para avaliar o estado de segurança do seu ambiente de acordo com os padrões e as melhores práticas do setor. Além de avaliar sua postura de segurança, o Security Hub CSPM cria um local central para descobertas em todos os seus AWS serviços integrados e produtos de parceiros. AWS A ativação do CSPM do Security Hub com GuardDuty permitirá automaticamente que os dados das GuardDuty descobertas sejam ingeridos pelo CSPM do Security Hub.

Para obter mais informações sobre como usar o Security Hub CSPM com GuardDuty , consulte. Integrar ao AWS Security Hub CSPM

Integração GuardDuty com o Amazon Detective

O Amazon Detective usa dados de log de todas AWS as suas contas para criar visualizações de dados para seus recursos e endereços IP que interagem com seu ambiente. As visualizações do Detective ajudam você a investigar problemas de segurança com rapidez e facilidade. Você pode passar da GuardDuty busca de detalhes para as informações no console do Detective quando os dois serviços estiverem ativados.

Para obter mais informações sobre como usar o Detective com GuardDuty , consulte. Integração com o Amazon Detective

Integrar ao AWS Security Hub CSPM

O AWS Security Hub CSPM fornece uma visão abrangente do estado de segurança na AWS e ajuda a verificar o ambiente em relação aos padrões e às práticas recomendadas do setor de segurança. O Security Hub CSPM coleta dados de segurança de várias AWS contas, serviços e produtos

de parceiros terceirizados compatíveis e ajuda você a analisar suas tendências de segurança e identificar os problemas de segurança de maior prioridade.

A GuardDuty integração da Amazon com o Security Hub CSPM permite que você envie descobertas para o Security Hub CSPM. GuardDuty O Security Hub CSPM pode então incluir essas descobertas em sua análise de sua postura de segurança.

Sumário

- Como a Amazon GuardDuty envia descobertas para AWS Security Hub CSPM
  - Tipos de descobertas GuardDuty enviadas ao CSPM do Security Hub
    - Latência para enviar descobertas
    - Nova tentativa quando o CSPM do Security Hub não está disponível
    - Atualização das descobertas existentes no CSPM do Security Hub
- Visualizando GuardDuty descobertas em AWS Security Hub CSPM
  - Interpretando GuardDuty encontrar nomes em AWS Security Hub CSPM
  - Descoberta típica de GuardDuty
- Habilitar e configurar a integração
- Usando GuardDuty controles no Security Hub CSPM
- Interrupção da publicação de descobertas no CSPM do Security Hub

Como a Amazon GuardDuty envia descobertas para AWS Security Hub CSPM

Em AWS Security Hub CSPM, os problemas de segurança são rastreados como descobertas. Algumas descobertas vêm de problemas detectados por outros AWS serviços ou por parceiros terceirizados. O CSPM do Security Hub também tem um conjunto de regras que ele usa para detectar problemas de segurança e gerar descobertas.

O CSPM do Security Hub fornece ferramentas para gerenciar descobertas em todas essas origens. É possível exibir e filtrar listas de descobertas e exibir detalhes de uma descoberta. Para obter mais informações, consulte Visualizar descobertas no Guia do usuário do AWS Security Hub . Também é possível rastrear o status de uma investigação em uma descoberta. Para obter mais informações, consulte Tomar medidas sobre descobertas no Manual do usuário do AWS Security Hub .

Todas as descobertas no Security Hub CSPM usam um formato JSON padrão chamado AWS Security Finding Format (ASFF). O ASFF inclui detalhes sobre a origem do problema, os recursos afetados e o status atual da descoberta. Consulte ASFF (Formato de Descoberta de Segurança) da AWS no Guia do usuário do AWS Security Hub .

A Amazon GuardDuty é um dos AWS serviços que envia descobertas para o Security Hub CSPM.

Tipos de descobertas GuardDuty enviadas ao CSPM do Security Hub

Depois de habilitar o GuardDuty Security Hub CSPM na mesma conta dentro da mesma Região da AWS, GuardDuty começa a enviar todas as descobertas geradas para o Security Hub CSPM. Essas descobertas são enviadas ao Security Hub CSPM usando o AWS Security Finding Format (ASFF). No ASFF, o campo `Types` fornece o tipo de descoberta.

Latência para enviar descobertas

Quando GuardDuty cria uma nova descoberta, ela geralmente é enviada ao CSPM do Security Hub em cinco minutos.

Nova tentativa quando o CSPM do Security Hub não está disponível

Se o CSPM do Security Hub não estiver disponível, GuardDuty tente enviar novamente as descobertas até que elas sejam recebidas.

Atualização das descobertas existentes no CSPM do Security Hub

Depois de enviar uma descoberta para o CSPM do Security Hub, GuardDuty envia atualizações para refletir observações adicionais da atividade de descoberta para o CSPM do Security Hub. As novas observações dessas descobertas são enviadas ao Security Hub CSPM com base nas Etapa 5 — Frequência de exportação de descobertas configurações do seu. Conta da AWS

Quando você arquiva ou desarquiva uma descoberta, GuardDuty não a envia para o CSPM do Security Hub. Qualquer descoberta desarquivada manualmente que posteriormente se torne ativa não GuardDuty é enviada ao CSPM do Security Hub.

Visualizando GuardDuty descobertas em AWS Security Hub CSPM

Faça login no Console de gerenciamento da AWS e abra o AWS Security Hub CSPM console em https://console.aws.amazon.com/securityhub/.

Agora você pode usar qualquer uma das seguintes formas de visualizar as GuardDuty descobertas no console CSPM do Security Hub:

Opção 1: Usando integrações no CSPM do Security Hub

1. No painel de navegação à esquerda, selecione Integrações.
2. Na página de integrações, verifique o status da Amazon: GuardDuty.
   - Se o Status for Aceitando descobertas, escolha Ver descobertas ao lado de Aceitar descobertas.
   - Caso contrário, para obter mais informações sobre como as integrações funcionam, consulte Integrações CSPM do Security Hub no Guia do Usuário.AWS Security Hub

Opção 2: Usando descobertas no CSPM do Security Hub

1. No painel de navegação à esquerda, escolha Descobertas.
2. Na página Descobertas, adicione o filtro Nome do produto e insira **`GuardDuty`** para ver somente GuardDuty as descobertas.

Interpretando GuardDuty encontrar nomes em AWS Security Hub CSPM

GuardDuty envia as descobertas para o Security Hub CSPM usando o AWS Security Finding Format (ASFF). No ASFF, o campo `Types` fornece o tipo de descoberta. Os tipos ASFF usam um esquema de nomenclatura diferente dos tipos. GuardDuty A tabela abaixo detalha todos os tipos de GuardDuty descobertas com seus equivalentes do ASFF conforme aparecem no CSPM do Security Hub.

> **Note**
>
> Para alguns tipos de GuardDuty descoberta, o Security Hub CSPM atribui nomes de descoberta ASFF diferentes, dependendo se a função de recurso do detalhe da descoberta era ACTOR ou TARGET. Para obter mais informações, consulte Detalhes da descoberta.

GuardDuty tipo de descoberta	Tipo de descoberta do ASFF
AttackSequence:IAM/CompromisedCredentials	TTPs/AttackSequence:IAM/CompromisedCredentials

GuardDuty tipo de descoberta	Tipo de descoberta do ASFF
AttackSequence:S3/CompromisedData	TTPs/AttackSequence:S3/CompromisedData
Backdoor:EC2/C&CActivity.B	TTPs/Command and Control/Backdoor:EC2-C&CActivity.B
Backdoor:EC2/C&CActivity.B!DNS	TTPs/Command and Control/Backdoor:EC2-C&CActivity.B!DNS
Backdoor:EC2/DenialOfService.Dns	TTPs/Command and Control/Backdoor:EC2-DenialOfService.Dns
Backdoor:EC2/DenialOfService.Tcp	TTPs/Command and Control/Backdoor:EC2-DenialOfService.Tcp
Backdoor:EC2/DenialOfService.Udp	TTPs/Command and Control/Backdoor:EC2-DenialOfService.Udp
Backdoor:EC2/DenialOfService.UdpOnTcpPorts	TTPs/Command and Control/Backdoor:EC2-DenialOfService.UdpOnTcpPorts
Backdoor:EC2/DenialOfService.UnusualProtocol	TTPs/Command and Control/Backdoor:EC2-DenialOfService.UnusualProtocol
Backdoor:EC2/Spambot	TTPs/Command and Control/Backdoor:EC2-Spambot
Behavior:EC2/NetworkPortUnusual	Unusual Behaviors/VM/Behavior:EC2-NetworkPortUnusual
Behavior:EC2/TrafficVolumeUnusual	Unusual Behaviors/VM/Behavior:EC2-TrafficVolumeUnusual
Backdoor:Lambda/C&CActivity.B	TTPs/Command and Control/Backdoor:Lambda-C&CActivity.B
Backdoor:Runtime/C&CActivity.B	TTPs/Command and Control/Backdoor:Runtime-C&CActivity.B

GuardDuty tipo de descoberta	Tipo de descoberta do ASFF
Backdoor:Runtime/C&CActivity.B!DNS	TTPs/Command and Control/Backdoor:Runtime-C&CActivity.B!DNS
CredentialAccess:IAMUser/AnomalousBehavior	TTPs/Credential Access/IAMUser-AnomalousBehavior
CredentialAccess:Kubernetes/AnomalousBehavior.SecretsAccessed	TTPs/AnomalousBehavior/CredentialAccess:Kubernetes-SecretsAccessed
CredentialAccess:Kubernetes/MaliciousIPCaller	TTPs/CredentialAccess/CredentialAccess:Kubernetes-MaliciousIPCaller
CredentialAccess:Kubernetes/MaliciousIPCaller.Custom	TTPs/CredentialAccess/CredentialAccess:Kubernetes-MaliciousIPCaller.Custom
CredentialAccess:Kubernetes/SuccessfulAnonymousAccess	TTPs/CredentialAccess/CredentialAccess:Kubernetes-SuccessfulAnonymousAccess
CredentialAccess:Kubernetes/TorIPCaller	TTPs/CredentialAccess/CredentialAccess:Kubernetes-TorIPCaller
CredentialAccess:RDS/AnomalousBehavior.FailedLogin	TTPs/Credential Access/CredentialAccess:RDS-AnomalousBehavior.FailedLogin
CredentialAccess:RDS/AnomalousBehavior.SuccessfulBruteForce	TTPs/Credential Access/CredentialAccess:RDS-AnomalousBehavior.SuccessfulBruteForce
CredentialAccess:RDS/AnomalousBehavior.SuccessfulLogin	TTPs/Credential Access/CredentialAccess:RDS-AnomalousBehavior.SuccessfulLogin
CredentialAccess:RDS/MaliciousIPCaller.FailedLogin	TTPs/Credential Access/CredentialAccess:RDS-MaliciousIPCaller.FailedLogin
CredentialAccess:RDS/MaliciousIPCaller.SuccessfulLogin	TTPs/Credential Access/CredentialAccess:RDS-MaliciousIPCaller.SuccessfulLogin
CredentialAccess:RDS/TorIPCaller.FailedLogin	TTPs/Credential Access/CredentialAccess:RDS-TorIPCaller.FailedLogin

GuardDuty tipo de descoberta	Tipo de descoberta do ASFF
CredentialAccess:RDS/TorIPCaller.SuccessfulLogin	TTPs/Credential Access/CredentialAccess:RDS-TorIPCaller.SuccessfulLogin
CryptoCurrency:EC2/BitcoinTool.B	TTPs/Command and Control/CryptoCurrency:EC2-BitcoinTool.B
CryptoCurrency:EC2/BitcoinTool.B!DNS	TTPs/Command and Control/CryptoCurrency:EC2-BitcoinTool.B!DNS
CryptoCurrency:Lambda/BitcoinTool.B	TTPs/Command and Control/CryptoCurrency:Lambda-BitcoinTool.B Effects/Resource Consumption/CryptoCurrency:Lambda-BitcoinTool.B
CommandAndControl:Runtime/SuspiciousCommand	TTPs/Command and Control/CommandAndControl:Runtime-SuspiciousCommand
CredentialAccess:Runtime/SensitiveFileRead	TTPs/Credential Access/CredentialAccess:Runtime-SensitiveFileRead
CryptoCurrency:Runtime/BitcoinTool.B	TTPs/Command and Control/CryptoCurrency:Runtime-BitcoinTool.B
CryptoCurrency:Runtime/BitcoinTool.B!DNS	TTPs/Command and Control/CryptoCurrency:Runtime-BitcoinTool.B!DNS
DefenseEvasion:EC2/UnusualDNSResolver	TTPs/DefenseEvasion/EC2:Unusual-DNS-Resolver
DefenseEvasion:EC2/UnusualDoHActivity	TTPs/DefenseEvasion/EC2:Unusual-DoH-Activity
DefenseEvasion:EC2/UnusualDoTActivity	TTPs/DefenseEvasion/EC2:Unusual-DoT-Activity
DefenseEvasion:IAMUser/AnomalousBehavior	TTPs/Defense Evasion/IAMUser-AnomalousBehavior

GuardDuty tipo de descoberta	Tipo de descoberta do ASFF
DefenseEvasion:IAMUser/BedrockLoggingDisabled	TTPs/Defense Evasion/DefenseEvasion:IAMUser-BedrockLoggingDisabled
DefenseEvasion:Kubernetes/MaliciousIPCaller	TTPs/DefenseEvasion/DefenseEvasion:Kubernetes-MaliciousIPCaller
DefenseEvasion:Kubernetes/MaliciousIPCaller.Custom	TTPs/DefenseEvasion/DefenseEvasion:Kubernetes-MaliciousIPCaller.Custom
DefenseEvasion:Kubernetes/SuccessfulAnonymousAccess	TTPs/DefenseEvasion/DefenseEvasion:Kubernetes-SuccessfulAnonymousAccess
DefenseEvasion:Kubernetes/TorIPCaller	TTPs/DefenseEvasion/DefenseEvasion:Kubernetes-TorIPCaller
DefenseEvasion:Runtime/FilelessExecution	TTPs/Defense Evasion/DefenseEvasion:Runtime-FilelessExecution
DefenseEvasion:Runtime/KernelModuleLoaded	TTPs/Defense Evasion/DefenseEvasion:Runtime-KernelModuleLoaded
DefenseEvasion:Runtime/SensitiveFileModified	TTPs/Defense Evasion/DefenseEvasion:Runtime-SensitiveFileModified
DefenseEvasion:Runtime/ProcessInjection.Proc	TTPs/Defense Evasion/DefenseEvasion:Runtime-ProcessInjection.Proc
DefenseEvasion:Runtime/ProcessInjection.Ptrace	TTPs/Defense Evasion/DefenseEvasion:Runtime-ProcessInjection.Ptrace
DefenseEvasion:Runtime/ProcessInjection.VirtualMemoryWrite	TTPs/Defense Evasion/DefenseEvasion:Runtime-ProcessInjection.VirtualMemoryWrite
DefenseEvasion:Runtime/PtraceAntiDebugging	TTPs/DefenseEvasion/DefenseEvasion:Runtime-PtraceAntiDebugging
DefenseEvasion:Runtime/SuspiciousCommand	TTPs/DefenseEvasion/DefenseEvasion:Runtime-SuspiciousCommand

GuardDuty tipo de descoberta	Tipo de descoberta do ASFF
Discovery:IAMUser/AnomalousBehavior	TTPs/Discovery/IAMUser-AnomalousBehavior
Discovery:Kubernetes/AnomalousBehavior.PermissionChecked	TTPs/AnomalousBehavior/Discovery:Kubernetes-PermissionChecked
Discovery:Kubernetes/MaliciousIPCaller	TTPs/Discovery/Discovery:Kubernetes-MaliciousIPCaller
Discovery:Kubernetes/MaliciousIPCaller.Custom	TTPs/Discovery/Discovery:Kubernetes-MaliciousIPCaller.Custom
Discovery:Kubernetes/SuccessfulAnonymousAccess	TTPs/Discovery/Discovery:Kubernetes-SuccessfulAnonymousAccess
Discovery:Kubernetes/TorIPCaller	TTPs/Discovery/Discovery:Kubernetes-TorIPCaller
Discovery:RDS/MaliciousIPCaller	TTPs/Discovery/RDS-MaliciousIPCaller
Discovery:RDS/TorIPCaller	TTPs/Discovery/RDS-TorIPCaller
Discovery:Runtime/SensitiveFileRead	TTPs/Discovery/Discovery:Runtime-SensitiveFileRead
Discovery:Runtime/SuspiciousCommand	TTPs/Discovery/Discovery:Runtime-SuspiciousCommand
Discovery:S3/AnomalousBehavior	TTPs/Discovery:S3-AnomalousBehavior
Discovery:S3/BucketEnumeration.Unusual	TTPs/Discovery:S3-BucketEnumeration.Unusual
Discovery:S3/MaliciousIPCaller.Custom	TTPs/Discovery:S3-MaliciousIPCaller.Custom
Discovery:S3/TorIPCaller	TTPs/Discovery:S3-TorIPCaller
Discovery:S3/MaliciousIPCaller	TTPs/Discovery:S3-MaliciousIPCaller
Exfiltration:IAMUser/AnomalousBehavior	TTPs/Exfiltration/IAMUser-AnomalousBehavior

GuardDuty tipo de descoberta	Tipo de descoberta do ASFF
Execution:Kubernetes/ExecInKubeSystemPod	TTPs/Execution/Execution:Kubernetes-ExecInKubeSystemPod
Execution:Kubernetes/AnomalousBehavior.ExecInPod	TTPs/AnomalousBehavior/Execution:Kubernetes-ExecInPod
Execution:Kubernetes/AnomalousBehavior.WorkloadDeployed	TTPs/AnomalousBehavior/Execution:Kubernetes-WorkloadDeployed
Impact:EC2/MaliciousDomainRequest.Custom	TTPs/Impact/Impact:EC2-MaliciousDomainRequest.Custom
Impact:Kubernetes/MaliciousIPCaller	TTPs/Impact/Impact:Kubernetes-MaliciousIPCaller
Impact:Kubernetes/MaliciousIPCaller.Custom	TTPs/Impact/Impact:Kubernetes-MaliciousIPCaller.Custom
Impact:Kubernetes/SuccessfulAnonymousAccess	TTPs/Impact/Impact:Kubernetes-SuccessfulAnonymousAccess
Impact:Kubernetes/TorIPCaller	TTPs/Impact/Impact:Kubernetes-TorIPCaller
Persistence:Kubernetes/ContainerWithSensitiveMount	TTPs/Persistence/Persistence:Kubernetes-ContainerWithSensitiveMount
Persistence:Kubernetes/AnomalousBehavior.WorkloadDeployed!ContainerWithSensitiveMount	TTPs/AnomalousBehavior/Persistence:Kubernetes-WorkloadDeployed!ContainerWithSensitiveMount
PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!PrivilegedContainer	TTPs/AnomalousBehavior/PrivilegeEscalation:Kubernetes-WorkloadDeployed!PrivilegedContainer
Persistence:Kubernetes/MaliciousIPCaller	TTPs/Persistence/Persistence:Kubernetes-MaliciousIPCaller

GuardDuty tipo de descoberta	Tipo de descoberta do ASFF
Persistence:Kubernetes/MaliciousIPCaller.Custom	TTPs/Persistence/Persistence:Kubernetes-MaliciousIPCaller.Custom
Persistence:Kubernetes/SuccessfulAnonymousAccess	TTPs/Persistence/Persistence:Kubernetes-SuccessfulAnonymousAccess
Persistence:Kubernetes/TorIPCaller	TTPs/Persistence/Persistence:Kubernetes-TorIPCaller
Execution:EC2/MaliciousFile	TTPs/Execution/Execution:EC2-MaliciousFile
Execution:ECS/MaliciousFile	TTPs/Execution/Execution:ECS-MaliciousFile
Execution:Kubernetes/MaliciousFile	TTPs/Execution/Execution:Kubernetes-MaliciousFile
Execution:Container/MaliciousFile	TTPs/Execution/Execution:Container-MaliciousFile
Execution:EC2/SuspiciousFile	TTPs/Execution/Execution:EC2-SuspiciousFile
Execution:ECS/SuspiciousFile	TTPs/Execution/Execution:ECS-SuspiciousFile
Execution:Kubernetes/SuspiciousFile	TTPs/Execution/Execution:Kubernetes-SuspiciousFile
Execution:Container/SuspiciousFile	TTPs/Execution/Execution:Container-SuspiciousFile
Execution:EC2/MaliciousFile!Snapshot	TTPs/Execution/Execution:EC2-MaliciousFile!Snapshot
Execution:EC2/MaliciousFile!AMI	TTPs/Execution/Execution:EC2-MaliciousFile!AMI
Execution:EC2/MaliciousFile!RecoveryPoint	TTPs/Execution/Execution:EC2-MaliciousFile!RecoveryPoint

GuardDuty tipo de descoberta	Tipo de descoberta do ASFF
Execution:S3/MaliciousFile!RecoveryPoint	TTPs/Execution/Execution:S3-MaliciousFile!RecoveryPoint
Execution:Runtime/MaliciousFileExecuted	TTPs/Execution/Execution:Runtime-MaliciousFileExecuted
Execution:Runtime/MaliciousFileExecuted.Custom	TTPs/Execution/Execution:Runtime-MaliciousFileExecuted.Custom
Execution:Runtime/NewBinaryExecuted	TTPs/Execution/Execution:Runtime-NewBinaryExecuted
Execution:Runtime/NewLibraryLoaded	TTPs/Execution/Execution:Runtime-NewLibraryLoaded
Execution:Runtime/ReverseShell	TTPs/Execution/Execution:Runtime-ReverseShell
Execution:Runtime/SuspiciousCommand	TTPs/Execution/Execution:Runtime-SuspiciousCommand
Execution:Runtime/SuspiciousShellCreated	TTPs/Execution/Execution:Runtime-SuspiciousShellCreated
Execution:Runtime/SuspiciousTool	TTPs/Execution/Execution:Runtime-SuspiciousTool
Exfiltration:S3/AnomalousBehavior	TTPs/Exfiltration:S3-AnomalousBehavior
Exfiltration:S3/ObjectRead.Unusual	TTPs/Exfiltration:S3-ObjectRead.Unusual
Exfiltration:S3/MaliciousIPCaller	TTPs/Exfiltration:S3-MaliciousIPCaller
Impact:EC2/AbusedDomainRequest.Reputation	TTPs/Impact:EC2-AbusedDomainRequest.Reputation
Impact:EC2/BitcoinDomainRequest.Reputation	TTPs/Impact:EC2-BitcoinDomainRequest.Reputation

GuardDuty tipo de descoberta	Tipo de descoberta do ASFF
Impact:EC2/MaliciousDomainRequest.Reputation	TTPs/Impact:EC2-MaliciousDomainRequest.Reputation
Impact:EC2/PortSweep	TTPs/Impact/Impact:EC2-PortSweep
Impact:EC2/SuspiciousDomainRequest.Reputation	TTPs/Impact:EC2-SuspiciousDomainRequest.Reputation
Impact:EC2/WinRMBruteForce	TTPs/Impact/Impact:EC2-WinRMBruteForce
Impact:IAMUser/AnomalousBehavior	TTPs/Impact/IAMUser-AnomalousBehavior
Exfiltration:Runtime/SuspiciousCommand	TTPs/Exfiltration/Exfiltration:Runtime-SuspiciousCommand
Impact:Runtime/AbusedDomainRequest.Reputation	TTPs/Impact/Impact:Runtime-AbusedDomainRequest.Reputation
Impact:Runtime/BitcoinDomainRequest.Reputation	TTPs/Impact/Impact:Runtime-BitcoinDomainRequest.Reputation
Impact:Runtime/CryptoMinerExecuted	TTPs/Impact/Impact:Runtime-CryptoMinerExecuted
Impact:Runtime/MaliciousDomainRequest.Reputation	TTPs/Impact/Impact:Runtime-MaliciousDomainRequest.Reputation
Impact:Runtime/SuspiciousDomainRequest.Reputation	TTPs/Impact/Impact:Runtime-SuspiciousDomainRequest.Reputatio
Impact:S3/AnomalousBehavior.Delete	TTPs/Impact:S3-AnomalousBehavior.Delete
Impact:S3/AnomalousBehavior.Permission	TTPs/Impact:S3-AnomalousBehavior.Permission
Impact:S3/AnomalousBehavior.Write	TTPs/Impact:S3-AnomalousBehavior.Write
Impact:S3/ObjectDelete.Unusual	TTPs/Impact:S3-ObjectDelete.Unusual

GuardDuty tipo de descoberta	Tipo de descoberta do ASFF
Impact:S3/PermissionsModification.Unusual	TTPs/Impact:S3-PermissionsModification.Unusual
Impact:S3/MaliciousIPCaller	TTPs/Impact:S3-MaliciousIPCaller
InitialAccess:IAMUser/AnomalousBehavior	TTPs/Initial Access/IAMUser-AnomalousBehavior
Object:S3/MaliciousFile	TTPs/Object/Object:S3-MaliciousFile
PenTest:IAMUser/KaliLinux	TTPs/PenTest:IAMUser/KaliLinux
PenTest:IAMUser/ParrotLinux	TTPs/PenTest:IAMUser/ParrotLinux
PenTest:IAMUser/PentooLinux	TTPs/PenTest:IAMUser/PentooLinux
PenTest:S3/KaliLinux	TTPs/PenTest:S3-KaliLinux
PenTest:S3/ParrotLinux	TTPs/PenTest:S3-ParrotLinux
PenTest:S3/PentooLinux	TTPs/PenTest:S3-PentooLinux
Persistence:IAMUser/AnomalousBehavior	TTPs/Persistence/IAMUser-AnomalousBehavior
Persistence:IAMUser/NetworkPermissions	TTPs/Persistence/Persistence:IAMUser-NetworkPermissions
Persistence:IAMUser/ResourcePermissions	TTPs/Persistence/Persistence:IAMUser-ResourcePermissions
Persistence:IAMUser/UserPermissions	TTPs/Persistence/Persistence:IAMUser-UserPermissions
Persistence:Runtime/SuspiciousCommand	TTPs/Persistence/Persistence:Runtime-SuspiciousCommand
Persistence:Runtime/SensitiveFileModified	TTPs/Persistence/Persistence:Runtime-SensitiveFileModified

GuardDuty tipo de descoberta	Tipo de descoberta do ASFF
Policy:IAMUser/RootCredentialUsage	TTPs/Policy:IAMUser-RootCredentialUsage
Policy:IAMUser/ShortTermRootCredentialUsage	TTPs/Policy:IAMUser-ShortTermRootCredentialUsage
Policy:Kubernetes/AdminAccessToDefaultServiceAccount	Software and Configuration Checks/AWS Security Best Practices/Policy:Kubernetes-AdminAccessToDefaultServiceAccount
Policy:Kubernetes/AnonymousAccessGranted	Software and Configuration Checks/AWS Security Best Practices/Policy:Kubernetes-AnonymousAccessGranted
Policy:Kubernetes/ExposedDashboard	Software and Configuration Checks/AWS Security Best Practices/Policy:Kubernetes-ExposedDashboard
Policy:Kubernetes/KubeflowDashboardExposed	Software and Configuration Checks/AWS Security Best Practices/Policy:Kubernetes-KubeflowDashboardExposed
Policy:S3/AccountBlockPublicAccessDisabled	TTPs/Policy:S3-AccountBlockPublicAccessDisabled
Policy:S3/BucketAnonymousAccessGranted	TTPs/Policy:S3-BucketAnonymousAccessGranted
Policy:S3/BucketBlockPublicAccessDisabled	Effects/Data Exposure/Policy:S3-BucketBlockPublicAccessDisabled
Policy:S3/BucketPublicAccessGranted	TTPs/Policy:S3-BucketPublicAccessGranted
PrivilegeEscalation:IAMUser/AnomalousBehavior	TTPs/Privilege Escalation/IAMUser-AnomalousBehavior
PrivilegeEscalation:IAMUser/AdministrativePermissions	TTPs/Privilege Escalation/PrivilegeEscalation:IAMUser-AdministrativePermissions

GuardDuty tipo de descoberta	Tipo de descoberta do ASFF
PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleBindingCreated	TTPs/AnomalousBehavior/PrivilegeEscalation:Kubernetes-RoleBindingCreated
PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleCreated	TTPs/AnomalousBehavior/PrivilegeEscalation:Kubernetes-RoleCreated
PrivilegeEscalation:Kubernetes/PrivilegedContainer	TTPs/PrivilegeEscalation/PrivilegeEscalation:Kubernetes-PrivilegedContainer
PrivilegeEscalation:Runtime/ContainerMountsHostDirectory	TTPs/Privilege Escalation/PrivilegeEscalation:Runtime-ContainerMountsHostDirectory
PrivilegeEscalation:Runtime/CGroupsReleaseAgentModified	TTPs/Privilege Escalation/PrivilegeEscalation:Runtime-CGroupsReleaseAgentModified
PrivilegeEscalation:Runtime/DockerSocketAccessed	TTPs/Privilege Escalation/PrivilegeEscalation:Runtime-DockerSocketAccessed
PrivilegeEscalation:Runtime/ElevationToRoot	TTPs/Privilege Escalation/PrivilegeEscalation:Runtime-ElevationToRoot
PrivilegeEscalation:Runtime/RuncContainerEscape	TTPs/Privilege Escalation/PrivilegeEscalation:Runtime-RuncContainerEscape
PrivilegeEscalation:Runtime/SuspiciousCommand	Software and Configuration Checks/PrivilegeEscalation:Runtime-SuspiciousCommand
PrivilegeEscalation:Runtime/SensitiveFileModified	TTPs/Privilege Escalation/PrivilegeEscalation:Runtime-SensitiveFileModified
PrivilegeEscalation:Runtime/UserfaultfdUsage	TTPs/Privilege Escalation/PrivilegeEscalation:Runtime-UserfaultfdUsage
Recon:EC2/PortProbeEMRUnprotectedPort	TTPs/Discovery/Recon:EC2-PortProbeEMRUnprotectedPort
Recon:EC2/PortProbeUnprotectedPort	TTPs/Discovery/Recon:EC2-PortProbeUnprotectedPort

GuardDuty tipo de descoberta	Tipo de descoberta do ASFF
Recon:EC2/Portscan	TTPs/Discovery/Recon:EC2-Portscan
Recon:IAMUser/MaliciousIPCaller	TTPs/Discovery/Recon:IAMUser-MaliciousIPCaller
Recon:IAMUser/MaliciousIPCaller.Custom	TTPs/Discovery/Recon:IAMUser-MaliciousIPCaller.Custom
Recon:IAMUser/NetworkPermissions	TTPs/Discovery/Recon:IAMUser-NetworkPermissions
Recon:IAMUser/ResourcePermissions	TTPs/Discovery/Recon:IAMUser-ResourcePermissions
Recon:IAMUser/TorIPCaller	TTPs/Discovery/Recon:IAMUser-TorIPCaller
Recon:IAMUser/UserPermissions	TTPs/Discovery/Recon:IAMUser-UserPermissions
ResourceConsumption:IAMUser/ComputeResources	Unusual Behaviors/User/ResourceConsumption:IAMUser-ComputeResources
Stealth:IAMUser/CloudTrailLoggingDisabled	TTPs/Defense Evasion/Stealth:IAMUser-CloudTrailLoggingDisabled
Stealth:IAMUser/LoggingConfigurationModified	TTPs/Defense Evasion/Stealth:IAMUser-LoggingConfigurationModified
Stealth:IAMUser/PasswordPolicyChange	TTPs/Defense Evasion/Stealth:IAMUser-PasswordPolicyChange
Stealth:S3/ServerAccessLoggingDisabled	TTPs/Defense Evasion/Stealth:S3-ServerAccessLoggingDisabled
Trojan:EC2/BlackholeTraffic	TTPs/Command and Control/Trojan:EC2-BlackholeTraffic

GuardDuty tipo de descoberta	Tipo de descoberta do ASFF
Trojan:EC2/BlackholeTraffic!DNS	TTPs/Command and Control/Trojan:EC2-BlackholeTraffic!DNS
Trojan:EC2/DGADomainRequest.B	TTPs/Command and Control/Trojan:EC2-DGADomainRequest.B
Trojan:EC2/DGADomainRequest.C!DNS	TTPs/Command and Control/Trojan:EC2-DGADomainRequest.C!DNS
Trojan:EC2/DNSDataExfiltration	TTPs/Command and Control/Trojan:EC2-DNSDataExfiltration
Trojan:EC2/DriveBySourceTraffic!DNS	TTPs/Initial Access/Trojan:EC2-DriveBySourceTraffic!DNS
Trojan:EC2/DropPoint	Effects/Data Exfiltration/Trojan:EC2-DropPoint
Trojan:EC2/DropPoint!DNS	Effects/Data Exfiltration/Trojan:EC2-DropPoint!DNS
Trojan:EC2/PhishingDomainRequest!DNS	TTPs/Command and Control/Trojan:EC2-PhishingDomainRequest!DNS
Trojan:Lambda/BlackholeTraffic	TTPs/Command and Control/Trojan:Lambda-BlackholeTraffic
Trojan:Lambda/DropPoint	Effects/Data Exfiltration/Trojan:Lambda-DropPoint
Trojan:Runtime/BlackholeTraffic	TTPs/Command and Control/Trojan:Runtime-BlackholeTraffic
Trojan:Runtime/BlackholeTraffic!DNS	TTPs/Command and Control/Trojan:Runtime-BlackholeTraffic!DNS
Trojan:Runtime/DGADomainRequest.C!DNS	TTPs/Command and Control/Trojan:Runtime-DGADomainRequest.C!DNS

GuardDuty tipo de descoberta	Tipo de descoberta do ASFF
Trojan:Runtime/DriveBySourceTraffic!DNS	TTPs/Initial Access/Trojan:Runtime-DriveBySourceTraffic!DNS
Trojan:Runtime/DropPoint	Effects/Data Exfiltration/Trojan:Runtime-DropPoint
Trojan:Runtime/DropPoint!DNS	Effects/Data Exfiltration/Trojan:Runtime-DropPoint!DNS
Trojan:Runtime/PhishingDomainRequest!DNS	TTPs/Command and Control/Trojan:Runtime-PhishingDomainRequest!DNS
UnauthorizedAccess:EC2/MaliciousIPCaller.Custom	TTPs/Command and Control/UnauthorizedAccess:EC2-MaliciousIPCaller.Custom
UnauthorizedAccess:EC2/MetadataDNSRebind	TTPs/UnauthorizedAccess:EC2-MetadataDNSRebind
UnauthorizedAccess:EC2/RDPBruteForce	TTPs/Initial Access/UnauthorizedAccess:EC2-RDPBruteForce
UnauthorizedAccess:EC2/SSHBruteForce	TTPs/Initial Access/UnauthorizedAccess:EC2-SSHBruteForce
UnauthorizedAccess:EC2/TorClient	Effects/Resource Consumption/UnauthorizedAccess:EC2-TorClient
UnauthorizedAccess:EC2/TorRelay	Effects/Resource Consumption/UnauthorizedAccess:EC2-TorRelay
UnauthorizedAccess:IAMUser/ConsoleLogin	Unusual Behaviors/User/UnauthorizedAccess:IAMUser-ConsoleLogin
UnauthorizedAccess:IAMUser/ConsoleLoginSuccess.B	TTPs/UnauthorizedAccess:IAMUser-ConsoleLoginSuccess.B

GuardDuty tipo de descoberta	Tipo de descoberta do ASFF
UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.InsideAWS	Effects/Data Exfiltration/UnauthorizedAccess:IAMUser-InstanceCredentialExfiltration.InsideAWS
UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS	Effects/Data Exfiltration/UnauthorizedAccess:IAMUser-InstanceCredentialExfiltration.OutsideAWS
UnauthorizedAccess:IAMUser/MaliciousIPCaller	TTPs/UnauthorizedAccess:IAMUser-MaliciousIPCaller
UnauthorizedAccess:IAMUser/MaliciousIPCaller.Custom	TTPs/UnauthorizedAccess:IAMUser-MaliciousIPCaller.Custom
UnauthorizedAccess:IAMUser/ResourceCredentialExfiltration.InsideAWS	Effects/Data Exfiltration/UnauthorizedAccess:IAMUser-ResourceCredentialExfiltration.InsideAWS
UnauthorizedAccess:IAMUser/ResourceCredentialExfiltration.OutsideAWS	Effects/Data Exfiltration/UnauthorizedAccess:IAMUser-ResourceCredentialExfiltration.OutsideAWS
UnauthorizedAccess:IAMUser/TorIPCaller	TTPs/Command and Control/UnauthorizedAccess:IAMUser-TorIPCaller
UnauthorizedAccess:Lambda/MaliciousIPCaller.Custom	TTPs/Command and Control/UnauthorizedAccess:Lambda-MaliciousIPCaller.Custom
UnauthorizedAccess:Lambda/TorClient	Effects/Resource Consumption/UnauthorizedAccess:Lambda-TorClient
UnauthorizedAccess:Lambda/TorRelay	Effects/Resource Consumption/UnauthorizedAccess:Lambda-TorRelay
UnauthorizedAccess:Runtime/MetadataDNSRebind	TTPs/UnauthorizedAccess:Runtime-MetadataDNSRebind

GuardDuty tipo de descoberta	Tipo de descoberta do ASFF
UnauthorizedAccess:Runtime/TorRelay	Effects/Resource Consumption/UnauthorizedAccess:Runtime-TorRelay
UnauthorizedAccess:Runtime/TorClient	Effects/Resource Consumption/UnauthorizedAccess:Runtime-TorClient
UnauthorizedAccess:S3/MaliciousIPCaller.Custom	TTPs/UnauthorizedAccess:S3-MaliciousIPCaller.Custom
UnauthorizedAccess:S3/TorIPCaller	TTPs/UnauthorizedAccess:S3-TorIPCaller

Descoberta típica de GuardDuty

GuardDuty envia descobertas para o Security Hub CSPM usando o AWS Security Finding Format (ASFF).

Aqui está um exemplo de uma descoberta típica de GuardDuty.


```
  {
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:guardduty:us-east-1:193043430472:detector/
d4b040365221be2b54a6264dc9a4bc64/finding/46ba0ac2845071e23ccdeb2ae03bfdea",
  "ProductArn": "arn:aws:securityhub:us-east-1:product/aws/guardduty",
  "GeneratorId": "arn:aws:guardduty:us-east-1:193043430472:detector/
d4b040365221be2b54a6264dc9a4bc64",
  "AwsAccountId": "193043430472",
  "Types": [
    "TTPs/Initial Access/UnauthorizedAccess:EC2-SSHBruteForce"
  ],
  "FirstObservedAt": "2020-08-22T09:15:57Z",
  "LastObservedAt": "2020-09-30T11:56:49Z",
  "CreatedAt": "2020-08-22T09:34:34.146Z",
  "UpdatedAt": "2020-09-30T12:14:00.206Z",
  "Severity": {
    "Product": 2,
    "Label": "MEDIUM",
    "Normalized": 40
  },
```

```
  "Title": "199.241.229.197 is performing SSH brute force attacks against
 i-0c10c2c7863d1a356.",
  "Description": "199.241.229.197 is performing SSH brute force attacks against
 i-0c10c2c7863d1a356. Brute force attacks are used to gain unauthorized access to your
 instance by guessing the SSH password.",
  "SourceUrl": "https://us-east-1.console.aws.amazon.com/guardduty/home?region=us-
east-1#/findings?macros=current&fId=46ba0ac2845071e23ccdeb2ae03bfdea",
  "ProductFields": {
    "aws/guardduty/service/action/networkConnectionAction/remotePortDetails/portName":
 "Unknown",
    "aws/guardduty/service/archived": "false",
    "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/organization/
asnOrg": "CENTURYLINK-US-LEGACY-QWEST",
    "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/geoLocation/
lat": "42.5122",
    "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/ipAddressV4":
 "199.241.229.197",
    "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/geoLocation/
lon": "-90.7384",
    "aws/guardduty/service/action/networkConnectionAction/blocked": "false",
    "aws/guardduty/service/action/networkConnectionAction/remotePortDetails/port":
 "46717",
    "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/country/
countryName": "United States",
    "aws/guardduty/service/serviceName": "guardduty",
    "aws/guardduty/service/evidence": "",
    "aws/guardduty/service/action/networkConnectionAction/localIpDetails/ipAddressV4":
 "172.31.43.6",
    "aws/guardduty/service/detectorId": "d4b040365221be2b54a6264dc9a4bc64",
    "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/organization/
org": "CenturyLink",
    "aws/guardduty/service/action/networkConnectionAction/connectionDirection":
 "INBOUND",
    "aws/guardduty/service/eventFirstSeen": "2020-08-22T09:15:57Z",
    "aws/guardduty/service/eventLastSeen": "2020-09-30T11:56:49Z",
    "aws/guardduty/service/action/networkConnectionAction/localPortDetails/portName":
 "SSH",
    "aws/guardduty/service/action/actionType": "NETWORK_CONNECTION",
    "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/city/
cityName": "Dubuque",
    "aws/guardduty/service/additionalInfo": "",
    "aws/guardduty/service/resourceRole": "TARGET",
    "aws/guardduty/service/action/networkConnectionAction/localPortDetails/port": "22",
    "aws/guardduty/service/action/networkConnectionAction/protocol": "TCP",
```

```
    "aws/guardduty/service/count": "74",
    "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/organization/
asn": "209",
    "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/organization/
isp": "CenturyLink",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/aws/guardduty/
arn:aws:guardduty:us-east-1:193043430472:detector/d4b040365221be2b54a6264dc9a4bc64/
finding/46ba0ac2845071e23ccdeb2ae03bfdea",
    "aws/securityhub/ProductName": "GuardDuty",
    "aws/securityhub/CompanyName": "Amazon"
  },
  "Resources": [
    {
      "Type": "AwsEc2Instance",
      "Id": "arn:aws:ec2:us-east-1:193043430472:instance/i-0c10c2c7863d1a356",
      "Partition": "aws",
      "Region": "us-east-1",
      "Tags": {
        "Name": "kubectl"
      },
      "Details": {
        "AwsEc2Instance": {
          "Type": "t2.micro",
          "ImageId": "ami-02354e95b39ca8dec",
          "IpV4Addresses": [
            "18.234.130.16",
            "172.31.43.6"
          ],
          "VpcId": "vpc-a0c2d7c7",
          "SubnetId": "subnet-4975b475",
          "LaunchedAt": "2020-08-03T23:21:57Z"
        }
      }
    }
  ],
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE"
}
```

Habilitar e configurar a integração

Para usar a integração com AWS Security Hub CSPM, você deve habilitar o CSPM do Security Hub. Para obter informações sobre como habilitar o Security Hub CSPM, consulte Configurar o Security Hub no Guia do usuário do AWS Security Hub .

Quando você ativa o CSPM do Security Hub GuardDuty e o Security Hub, a integração é ativada automaticamente. GuardDutyimediatamente começa a enviar as descobertas para o Security Hub CSPM.

Usando GuardDuty controles no Security Hub CSPM

AWS Security Hub CSPM usa controles de segurança para avaliar seus AWS recursos e verificar sua conformidade com os padrões e as melhores práticas do setor de segurança. Você pode usar os controles relacionados aos GuardDuty recursos e aos planos de proteção selecionados. Para obter mais informações, consulte GuardDutyos controles da Amazon no Guia AWS Security Hub do usuário.

Para obter uma lista de todos os controles entre AWS serviços e recursos, consulte a referência de controles CSPM do Security Hub no Guia do AWS Security Hub Usuário.

Interrupção da publicação de descobertas no CSPM do Security Hub

Para interromper o envio de descobertas ao CSPM do Security Hub, você poderá usar o console ou a API do CSPM do Security Hub.

Consulte Desabilitar e habilitar o fluxo de descobertas de uma integração (console) ou Desabilitar o fluxo de descobertas de uma integração (API do Security Hub, AWS CLI) no Guia do Usuário.AWS Security Hub

Integração com o Amazon Detective

O Amazon Detective ajuda você a analisar e investigar rapidamente eventos de segurança em uma ou mais AWS contas, gerando visualizações de dados que representam a forma como seus recursos se comportam e interagem ao longo do tempo. Detective cria visualizações das descobertas. GuardDuty

O Detective ingere detalhes de descoberta para todos os tipos de descoberta e fornece acesso aos perfis de entidades para investigar diferentes entidades envolvidas na descoberta. Uma entidade

pode ser um Conta da AWS AWS recurso dentro de uma conta ou um endereço IP externo que tenha interagido com seus recursos. O GuardDuty console suporta a migração para o Amazon Detective a partir das seguintes entidades, dependendo do tipo de descoberta Conta da AWS: função do IAM, usuário ou sessão de função, agente do usuário, usuário federado, instância do Amazon EC2 ou endereço IP.

Sumário

- Habilitar a integração
- Passando para o Amazon Detective a partir de uma descoberta GuardDuty
- Usando a integração com um ambiente de GuardDuty várias contas

Habilitar a integração

Para usar o Amazon Detective com GuardDuty você deve primeiro habilitar o Amazon Detective. Para informações sobre como habilitar o Detective, consulte Introdução ao Amazon Detective no Guia do usuário do Amazon Detective.

Quando você ativa o Detective GuardDuty e o Detective, a integração é ativada automaticamente. Depois de ativado, o Detective ingerirá imediatamente os dados de suas GuardDuty descobertas.

> **Note**
>
> GuardDuty envia as descobertas ao Detective com base na frequência de exportação das GuardDuty descobertas. Por padrão, a frequência de exportação para atualizações das descobertas existentes é de 6 horas. Para garantir que o Detective receba as atualizações mais recentes de suas descobertas, é recomendável alterar a frequência de exportação para 15 minutos em cada região em que você usa o Detective. GuardDuty Para obter mais informações, consulte Etapa 5: Definir a frequência para exportar descobertas ativas atualizadas.

Passando para o Amazon Detective a partir de uma descoberta GuardDuty

1. Faça login no https://console.aws.amazon.com/guardduty/console.
2. Selecione uma única descoberta da sua tabela de descobertas.
3. Selecione Investigar com Detective no painel de detalhes da descoberta.

4. Selecione um aspecto da descoberta para investigar com o Amazon Detective. Isso abre o console do Detective para essa descoberta ou entidade.

Se o pivô não se comportar conforme o esperado, consulte Solução de problemas do pivô no Guia do usuário do Amazon Detective.

> **Note**
>
> Se você arquivar uma GuardDuty descoberta no console do Detective, essa descoberta também será arquivada no GuardDuty console.

Usando a integração com um ambiente de GuardDuty várias contas

Se você estiver gerenciando um ambiente de várias contas em GuardDuty, você deve adicionar suas contas de membros ao Amazon Detective para visualizar visualizações de dados de Detective para descobertas e entidades nessas contas.

É recomendável que você use a mesma conta de GuardDuty administrador que a conta de administrador de Detective. Para obter mais informações sobre como adicionar contas de membros no Detective, consulte Gerenciamento de contas no Guia do usuário do Amazon Detective.

> **Note**
>
> Detective é um serviço regional, o que significa que você deve habilitar o Detective e adicionar suas contas-membro em cada região na qual deseja usar a integração.

Suspensão ou desativação GuardDuty

Você pode usar o GuardDuty console para suspender ou desativar o GuardDuty serviço. Você não é cobrado pelo uso GuardDuty quando o serviço é suspenso.

- Todas as contas dos membros devem ser desassociadas ou excluídas antes que você possa suspendê-las ou desativá-las. GuardDuty
- Se você suspender GuardDuty, ele não monitora mais a segurança do seu AWS ambiente nem gera novas descobertas. Suas descobertas existentes permanecem intactas e não são afetadas pela GuardDuty suspensão. Você pode optar por reativar GuardDuty mais tarde.
- Quando você desativa GuardDuty em uma conta, ela será desativada somente para a atualmente selecionada Região da AWS. Se você quiser desativá-lo completamente GuardDuty, você deve desativá-lo em cada região em que ele está ativado.
- Se você desabilitar GuardDuty, suas descobertas e a GuardDuty configuração existentes serão perdidas e não poderão ser recuperadas. Se quiser salvar suas descobertas existentes, você deve exportá-las antes de confirmar a desativação GuardDuty. Para obter informações sobre como exportar descobertas, consulte Exportar as descobertas geradas para bucket do Amazon S3.
- Se você ativou o Malware Protection for S3 para um ou mais buckets protegidos em sua conta, suspender ou desabilitar GuardDuty não afetará o status de um bucket protegido em Malware Protection for S3. Mesmo depois de suspender ou desativar GuardDuty, sua conta continuará incorrendo nos custos de uso associados ao recurso Malware Protection for S3. Para obter mais informações sobre como desabilitar a Proteção contra malware para o S3, consulte Desativando a proteção contra malware para S3 em um bucket protegido.

Para suspender ou desativar GuardDuty

1. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.
2. No painel de navegação, selecione Configurações.
3. Na GuardDuty seção Suspender, escolha Suspender GuardDuty ou Desativar e, em seguida GuardDuty, Confirme sua ação.

Para reativar GuardDuty após a suspensão

1. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.
2. No painel de navegação, selecione Configurações.

3. Selecione Re-enable GuardDuty.

Inscrever-se para receber anúncios do Amazon GuardDuty SNS

Esta seção fornece informações sobre a assinatura do Amazon SNS (Simple Notification Service) GuardDuty para receber anúncios sobre tipos de descoberta recém-lançados, atualizações dos tipos de descoberta existentes e outras alterações de funcionalidade. As notificações estão disponíveis em todos os formatos compatíveis com o Amazon SNS.

O GuardDuty SNS envia anúncios sobre atualizações do GuardDuty serviço AWS para qualquer conta assinada. Para receber notificações sobre descobertas em sua conta, consulte Processando GuardDuty descobertas com a Amazon EventBridge.

> **Note**
>
> Seu usuário do IAM deve ter permissões `sns::subscribe` para a inscrição em um SNS.

É possível se inscrever uma fila do Amazon SQS neste tópico de notificação, mas deve-se usar um ARN de tópico que esteja na mesma região. Para obter mais informações, consulte Tutorial: Inscrever-se em uma fila do Amazon SQS para um tópico do Amazon SNS no Guia do desenvolvedor do Amazon Simple Queue Service.

Você também pode usar uma AWS Lambda função para acionar eventos quando as notificações são recebidas. Para obter mais informações, consulte Invocar funções do Lambda usando notificações do Amazon SNS no Guia do desenvolvedor do Amazon Simple Queue Service.

Os ARNs do tópico do Amazon SNS de cada região são mostrados abaixo.

Região da AWS	Tópico ARN do Amazon SNS
Leste dos EUA (Norte da Virgínia): `us-east-1`	`arn:aws:sns:us-east-1:242987662583:GuardDutyAnnouncements`
Leste dos EUA (Ohio) - `us-east-2`	`arn:aws:sns:us-east-2:118283430703:G`

Região da AWS	Tópico ARN do Amazon SNS
	uardDutyAnnounceme nts
Oeste dos EUA (Norte da Califórnia) - us-west-1	arn:aws:sns:us-wes t-1:144182107116:G uardDutyAnnounceme nts
Oeste dos EUA (Oregon): us-west-2	arn:aws:sns:us-wes t-2:934957504740:G uardDutyAnnounceme nts
Canadá (Central) - ca-central-1	arn:aws:sns:ca-cen tral-1:10743005193 3:GuardDutyAnnounc ements
Oeste do Canadá (Calgary) - ca-west-1	arn:aws:sns:ca-wes t-1:440427180217:G uardDutyAnnounceme nts
Europa (Estocolmo) - eu-north-1	arn:aws:sns:eu-nor th-1:973841112453: GuardDutyAnnouncem ents
Europa (Irlanda) - eu-west-1	arn:aws:sns:eu-wes t-1:965013871422:G uardDutyAnnounceme nts

Região da AWS	Tópico ARN do Amazon SNS
Europa (Londres) - `eu-west-2`	`arn:aws:sns:eu-west-2:506403581195:GuardDutyAnnouncements`
Europa (Paris) - `eu-west-3`	`arn:aws:sns:eu-west-3:436163563069:GuardDutyAnnouncements`
Europa (Frankfurt) - `eu-central-1`	`arn:aws:sns:eu-central-1:378365507264:GuardDutyAnnouncements`
Europa (Zurique) - `eu-central-2`	`arn:aws:sns:eu-central-2:383009515534:GuardDutyAnnouncements`
Ásia-Pacífico (Hong Kong) - `ap-east-1`	`arn:aws:sns:ap-east-1:646602203151:GuardDutyAnnouncements`
Ásia-Pacífico (Tóquio): `ap-northeast-1`	`arn:aws:sns:ap-northeast-1:741172661024:GuardDutyAnnouncements`
Ásia-Pacífico (Seul) - `ap-northeast-2`	`arn:aws:sns:ap-northeast-2:464168911255:GuardDutyAnnouncements`

Região da AWS	Tópico ARN do Amazon SNS
Ásia-Pacífico (Singapura) - ap-southeast-1	arn:aws:sns:ap-southeast-1:476419727788:GuardDutyAnnouncements
Ásia-Pacífico (Sydney) - ap-southeast-2	arn:aws:sns:ap-southeast-2:457615622431:GuardDutyAnnouncements
Ásia-Pacífico (Mumbai) - ap-south-1	arn:aws:sns:ap-south-1:926826061926:GuardDutyAnnouncements
América do Sul (São Paulo) - sa-east-1	arn:aws:sns:sa-east-1:955633302743:GuardDutyAnnouncements
AWS GovCloud (US-West) - us-gov-west-1	arn:aws-us-gov:sns:us-gov-west-1:430639793359:GuardDutyAnnouncements
China (Pequim) - cn-north-1	arn:aws-cn:sns:cn-north-1:002991280229:GuardDutyAnnouncements
China (Ningxia) - cn-northwest-1	arn:aws-cn:sns:cn-northwest-1:003033775354:GuardDutyAnnouncements

Região da AWS	Tópico ARN do Amazon SNS
Oriente Médio (Bahrein) - me-south-1	arn:aws:sns:me-south-1:552740612889:GuardDutyAnnouncements
Oriente Médio (EAU) - me-central-1	arn:aws:sns:me-central-1:030935290150:GuardDutyAnnouncements
Europa (Milão) - eu-south-1	arn:aws:sns:eu-south-1:188461706213:GuardDutyAnnouncements
Europa (Espanha) - eu-south-2	arn:aws:sns:eu-south-2:445632894446:GuardDutyAnnouncements
AWS GovCloud (US-East) - us-gov-east-1	arn:aws:sns:us-gov-east-1:143972945659:GuardDutyAnnouncements
Asia Pacific (Osaka) - ap-northeast-3	arn:aws:sns:ap-northeast-3:129086577509:GuardDutyAnnouncements
Ásia-Pacífico (Jacarta) - ap-southeast-3	arn:aws:sns:ap-southeast-3:225965583551:GuardDutyAnnouncements

Região da AWS	Tópico ARN do Amazon SNS
Ásia-Pacífico (Hyderabad) - ap-south-2	arn:aws:sns:ap-south-2:595653072700:GuardDutyAnnouncements
Ásia-Pacífico (Melbourne) - ap-southeast-4	arn:aws:sns:ap-southeast-4:529900636122:GuardDutyAnnouncements
Ásia-Pacífico (Malásia) - ap-southeast-5	arn:aws:sns:ap-southeast-5:343218181797:GuardDutyAnnouncements
Israel (Tel Aviv) - il-central-1	arn:aws:sns:il-central-1:847886274986:GuardDutyAnnouncements
Ásia-Pacífico (Tailândia) - ap-southeast-7	arn:aws:sns:ap-southeast-7:863518448376:GuardDutyAnnouncements
México (Central) - mx-central-1	arn:aws:sns:mx-central-1:060795916546:GuardDutyAnnouncements
Ásia-Pacífico (Taipei) - ap-east-2	arn:aws:sns:ap-east-2:604225987917:GuardDutyAnnouncements

Para assinar o e-mail de notificação de GuardDuty atualização no Console de gerenciamento da AWS

1. Abra o console do Amazon SNS em https://console.aws.amazon.com/sns/v3/home.
2. Na lista de regiões, escolha a mesma região que o ARN do tópico que deseja assinar. Este exemplo usa a região `us-west-2`.
3. No painel de navegação à esquerda, escolha Assinaturas, Criar assinatura.
4. Na caixa de diálogo Criar assinatura, em ARN do tópico, cole o ARN do tópico: `arn:aws:sns:us-west-2:934957504740:GuardDutyAnnouncements`.
5. Em Protocolo, escolha E-mail. Em Endpoint, digite um endereço de e-mail que possa usado para receber a notificação.
6. Selecione Criar assinatura.
7. Em seu aplicativo de e-mail, abra a mensagem em AWS Notificações e abra o link para confirmar sua assinatura.

   O navegador da Web exibe uma resposta de confirmação do Amazon SNS.

Para assinar o e-mail de notificação de GuardDuty atualização com o AWS CLI

1. Execute o seguinte comando com a AWS CLI:

```
 aws  sns --region us-west-2 subscribe --topic-arn arn:aws:sns:us-
west-2:934957504740:GuardDutyAnnouncements --protocol email --notification-
endpoint your_email@your_domain.com
```

2. Em seu aplicativo de e-mail, abra a mensagem em AWS Notificações e abra o link para confirmar sua assinatura.

   O navegador da Web exibe uma resposta de confirmação do Amazon SNS.

Formato da mensagem do Amazon SNS

Um exemplo de mensagem de notificação GuardDuty geral:

```
{
    "Type" : "Notification",
    "MessageId" : "9101dc6b-726f-4df0-8646-ec2f94e674bc",
```

```
    "TopicArn" : "arn:aws:sns:us-west-2:934957504740:GuardDutyAnnouncements",
    "Message" : "{\"version\":\"1\",\"type\":\"GENERAL\",\"message\":[{\"title\":
\"Updated AmazonGuardDutyFullAccess_v2 policy\",\"body\":\"Added permission that
 allows you to pass an IAM role to GuardDuty when you enable Malware Protection for
 S3.\",\"links\":[\"https://docs.aws.amazon.com//guardduty/latest/ug/security-iam-
awsmanpol.html#security-iam-awsmanpol-AmazonGuardDutyFullAccess-v2\"]}]}",
    "Timestamp" : "2018-03-09T00:25:43.483Z",
    "SignatureVersion" : "1",
    "Signature" : "XWox8GDGLRiCgDOXlo/
fG9Lu/88P8S0FL6M6oQYOmUFzkucuhoblsdea3BjqdCHcWR7qdhMPQnLpN7y9iBrWVUqdAGJrukAI8athvAS
+4AQD/V/QjrhsEnlj+GaiW
+ozAu006X6GopOzFGnCtPMROjCMrMonjz7Hpv/8KRuMZR3pyQYm5d4wWB7xBPYhUMuLoZ1V8YFs55FMtgQV/
YLhSYuEu0BP1GMtLQauxDkscOtPP/vjhGQLFx1Q9LTadcQiRHtNIBxWL87PSI
+BVvkin6AL7PhksvdQ7FAgHfXsit+6p8GyOvKCqaeBG7HZhR1AbpyVka7JSNRO/6ssyrlj1g==",
    "SigningCertURL" : "https://sns.us-west-2.amazonaws.com/
SimpleNotificationService-433026a4050d206028891664da859041.pem",
    "UnsubscribeURL" : "https://sns.us-west-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-
west-2:934957504740:GuardDutyAnnouncements:9225ed2b-7228-4665-8a01-c8a5db6859f4"
}
```

O valor da mensagem analisada (sem aspas com escape) é mostrado abaixo:

```
{
        "version": "1",
        "type": "GENERAL",
        "message": [
            {
                "title": "Updated AmazonGuardDutyFullAccess policy",
                "body": "Added permission that allows you to pass an IAM role to
 GuardDuty when you enable Malware Protection for S3.",
                "links": [
                    "https://docs.aws.amazon.com//guardduty/latest/ug/security-iam-
awsmanpol.html#security-iam-awsmanpol-AmazonGuardDutyFullAccess-v2"
                ]
             }
        ]
}
```

Um exemplo de mensagem de notificação de GuardDuty atualização sobre novas descobertas é mostrado abaixo:

```
{
```

```
    "Type" : "Notification",
    "MessageId" : "9101dc6b-726f-4df0-8646-ec2f94e674bc",
    "TopicArn" : "arn:aws:sns:us-west-2:934957504740:GuardDutyAnnouncements",
    "Message" : "{\"version\":\"1\",\"type\":\"NEW_FINDINGS\",\"findingDetails
\":[{\"link\":\"https://docs.aws.amazon.com//guardduty/latest/ug/
guardduty_unauthorized.html\",\"findingType\":\"UnauthorizedAccess:EC2/TorClient\",
\"findingDescription\":\"This finding informs you that an EC2 instance in your AWS
 environment is making connections to a Tor Guard or an Authority node. Tor is software
 for enabling anonymous communication. Tor Guards and Authority nodes act as initial
 gateways into a Tor network. This traffic can indicate that this EC2 instance is
 acting as a client on a Tor network. A common use for a Tor client is to circumvent
 network monitoring and filter for access to unauthorized or illicit content. Tor
 clients can also generate nefarious Internet traffic, including attacking SSH servers.
 This activity can indicate that your EC2 instance is compromised.\"}]}",
    "Timestamp" : "2018-03-09T00:25:43.483Z",
    "SignatureVersion" : "1",
    "Signature" : "XWox8GDGLRiCgDOXlo/
fG9Lu/88P8S0FL6M6oQYOmUFzkucuhoblsdea3BjqdCHcWR7qdhMPQnLpN7y9iBrWVUqdAGJrukAI8athvAS
+4AQD/V/QjrhsEnlj+GaiW
+ozAu006X6GopOzFGnCtPMROjCMrMonjz7Hpv/8KRuMZR3pyQYm5d4wWB7xBPYhUMuLoZ1V8YFs55FMtgQV/
YLhSYuEu0BP1GMtLQauxDkscOtPP/vjhGQLFx1Q9LTadcQiRHtNIBxWL87PSI
+BVvkin6AL7PhksvdQ7FAgHfXsit+6p8GyOvKCqaeBG7HZhR1AbpyVka7JSNRO/6ssyrlj1g==",
    "SigningCertURL" : "https://sns.us-west-2.amazonaws.com/
SimpleNotificationService-433026a4050d206028891664da859041.pem",
    "UnsubscribeURL" : "https://sns.us-west-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-
west-2:934957504740:GuardDutyAnnouncements:9225ed2b-7228-4665-8a01-c8a5db6859f4"
}
```

O valor da mensagem analisada (sem aspas com escape) é mostrado abaixo:

```
{
    "version": "1",
    "type": "NEW_FINDINGS",
    "findingDetails": [{
        "link": "https://docs.aws.amazon.com//guardduty/latest/ug/
guardduty_unauthorized.html",
        "findingType": "UnauthorizedAccess:EC2/TorClient",
        "findingDescription": "This finding informs you that an EC2 instance in your
 AWS environment is making connections to a Tor Guard or an Authority node. Tor is
 software for enabling anonymous communication. Tor Guards and Authority nodes act as
 initial gateways into a Tor network. This traffic can indicate that this EC2 instance
 is acting as a client on a Tor network. A common use for a Tor client is to circumvent
```

```
 network monitoring and filter for access to unauthorized or illicit content. Tor
 clients can also generate nefarious Internet traffic, including attacking SSH servers.
 This activity can indicate that your EC2 instance is compromised."
    }]
}
```

Um exemplo de mensagem de notificação de GuardDuty atualização sobre atualizações de GuardDuty funcionalidade é mostrado abaixo:

```
{
    "Type" : "Notification",
    "MessageId" : "9101dc6b-726f-4df0-8646-ec2f94e674bc",
    "TopicArn" : "arn:aws:sns:us-west-2:934957504740:GuardDutyAnnouncements",
    "Message" : "{\"version\":\"1\",\"type\":\"NEW_FEATURES\",\"featureDetails
\":[{\"featureDescription\":\"Customers with high-volumes of global CloudTrail
 events should see a net positive impact on their GuardDuty costs.\",\"featureLink
\":\"https://docs.aws.amazon.com//guardduty/latest/ug/guardduty_data-
sources.html#guardduty_controlplane\"}]}",
    "Timestamp" : "2018-03-09T00:25:43.483Z",
    "SignatureVersion" : "1",
    "Signature" : "XWox8GDGLRiCgDOXlo/
fG9Lu/88P8S0FL6M6oQYOmUFzkucuhoblsdea3BjqdCHcWR7qdhMPQnLpN7y9iBrWVUqdAGJrukAI8athvAS
+4AQD/V/QjrhsEnlj+GaiW
+ozAu006X6GopOzFGnCtPMROjCMrMonjz7Hpv/8KRuMZR3pyQYm5d4wWB7xBPYhUMuLoZ1V8YFs55FMtgQV/
YLhSYuEu0BP1GMtLQauxDkscOtPP/vjhGQLFx1Q9LTadcQiRHtNIBxWL87PSI
+BVvkin6AL7PhksvdQ7FAgHfXsit+6p8GyOvKCqaeBG7HZhR1AbpyVka7JSNRO/6ssyrlj1g==",
    "SigningCertURL" : "https://sns.us-west-2.amazonaws.com/
SimpleNotificationService-433026a4050d206028891664da859041.pem",
    "UnsubscribeURL" : "https://sns.us-west-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-
west-2:934957504740:GuardDutyAnnouncements:9225ed2b-7228-4665-8a01-c8a5db6859f4"
}
```

O valor da mensagem analisada (sem aspas com escape) é mostrado abaixo:

```
{
    "version": "1",
    "type": "NEW_FEATURES",
    "featureDetails": [{
        "featureDescription": "Customers with high-volumes of global CloudTrail events
 should see a net positive impact on their GuardDuty costs.",
        "featureLink": "https://docs.aws.amazon.com//guardduty/latest/ug/
guardduty_data-sources.html#guardduty_controlplane"
```

```
    }]
}
```

Um exemplo de mensagem de notificação de GuardDuty atualização sobre descobertas atualizadas é mostrado abaixo:

```
{
    "Type": "Notification",
    "MessageId": "9101dc6b-726f-4df0-8646-ec2f94e674bc",
    "TopicArn": "arn:aws:sns:us-west-2:934957504740:GuardDutyAnnouncements",
    "Message": "{\"version\":\"1\",\"type\":\"UPDATED_FINDINGS\",
\"findingDetails\":[{\"link\":\"https://docs.aws.amazon.com//guardduty/latest/ug/
guardduty_unauthorized.html\",\"findingType\":\"UnauthorizedAccess:EC2/TorClient\",
\"description\":\"Increased severity value from 5 to 8.\"}]}",
    "Timestamp": "2018-03-09T00:25:43.483Z",
    "SignatureVersion": "1",
    "Signature": "XWox8GDGLRiCgDOXlo/
fG9Lu/88P8S0FL6M6oQYOmUFzkucuhoblsdea3BjqdCHcWR7qdhMPQnLpN7y9iBrWVUqdAGJrukAI8athvAS
+4AQD/V/QjrhsEnlj+GaiW
+ozAu006X6GopOzFGnCtPMROjCMrMonjz7Hpv/8KRuMZR3pyQYm5d4wWB7xBPYhUMuLoZ1V8YFs55FMtgQV/
YLhSYuEu0BP1GMtLQauxDkscOtPP/vjhGQLFx1Q9LTadcQiRHtNIBxWL87PSI
+BVvkin6AL7PhksvdQ7FAgHfXsit+6p8GyOvKCqaeBG7HZhR1AbpyVka7JSNRO/6ssyrlj1g==",
    "SigningCertURL": "https://sns.us-west-2.amazonaws.com/
SimpleNotificationService-433026a4050d206028891664da859041.pem",
    "UnsubscribeURL": "https://sns.us-west-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-
west-2:934957504740:GuardDutyAnnouncements:9225ed2b-7228-4665-8a01-c8a5db6859f4"
}
```

O valor da mensagem analisada (sem aspas com escape) é mostrado abaixo:

```
{
    "version": "1",
    "type": "UPDATED_FINDINGS",
    "findingDetails": [{
        "link": "https://docs.aws.amazon.com//guardduty/latest/ug/
guardduty_unauthorized.html",
        "findingType": "UnauthorizedAccess:EC2/TorClient",
        "description": "Increased severity value from 5 to 8."
    }]
}
```

GuardDuty Cotas da Amazon

Você Conta da AWS tem cotas padrão, anteriormente chamadas de limites, para cada um. AWS service (Serviço da AWS) Salvo indicação em contrário, cada cota é Region-specific. É possível solicitar aumentos para algumas cotas, enquanto outras cotas não podem ser aumentadas.

Para ver as cotas de GuardDuty, abra o console Service Quotas. No painel de navegação, escolha Serviços da AWSe selecione Amazon GuardDuty.

Para solicitar um aumento da cota, consulte Requesting a quota increase no Guia do usuário do Service Quotas.

Você Conta da AWS tem as seguintes cotas para a Amazon GuardDuty por região.

> **Note**
>
> - Para cotas específicas da Proteção contra GuardDuty Malware para EC2, consulte. Cotas na Proteção contra malware para o EC2
> - Para cotas específicas da Proteção contra malware para o EC3, consulte Quotas na Proteção contra malware para o S3.

GuardDuty cotas por região

Recurso	Padrão	Comentários
Detectores	1	O número máximo de recursos do detector que pode ser criado por conta da AWS e por região. Não é possível solicitar um aumento de cota.
Filtros	100	O número máximo de filtros salvos por AWS conta por região.

Recurso	Padrão	Comentários
		Não é possível solicitar um aumento de cota.
Período de retenção da descoberta	90 dias	O número máximo de dias em que uma descoberta é armazenada. Não é possível solicitar um aumento de cota.
Endereços IP e intervalos de CIDR por lista de endereços IP confiáveis	2.000	O número máximo de endereços IP e intervalos de CIDR que podem ser incluídos em uma única lista de endereços IP confiáveis. Não é possível solicitar um aumento de cota.

Recurso	Padrão	Comentários
Endereços IP e intervalos de CIDR por lista de endereços IP de ameaças	250.000	O número máximo de endereços IP e intervalos de CIDR que podem ser incluídos em uma lista de endereços IP de ameaças. Não é possível solicitar um aumento de cota.
Entidades por lista de entidades de ameaças	1.000	O número máximo de entidades que podem ser incluídas em uma única lista de entidades de ameaças. Não é possível solicitar um aumento de cota.
Entidades por lista de entidades confiáveis	1.000	O número máximo de entidades que podem ser incluídas em uma lista de entidades confiáveis. Não é possível solicitar um aumento de cota.

Recurso	Padrão	Comentários
Tamanho máximo do arquivo	35 MB	O tamanho máximo do arquivo usado para carregar uma lista de entidades ou uma lista de endereços IP. Não é possível solicitar um aumento de cota.
Contas de membros (por convite)	5000	O número máximo de contas de membros associadas a uma conta de administr ador. Não é possível solicitar um aumento de cota.

Recurso	Padrão	Comentários
Contas de membros	50.000	O número máximo de contas de membros associadas a uma conta de administrador por meio do AWS Organizations. Isso inclui contas de membros que são adicionadas à organização por convite. Esse valor padrão depende da sua cota atual para contas-membro em AWS Organizations. O número de contas de membros GuardDuty que são adicionadas por meio de não AWS Organizations pode exceder o número de contas de membros em sua organização. Para obter informações sobre o número de Contas da AWS em uma organização, consulte Valores máximos e mínimos no Guia AWS Organizations do usuário.

Recurso	Padrão	Comentários
Conjuntos de informações sobre ameaças (lista de endereços IP)	6	O número máximo de listas de endereços IP de ameaças que você pode adicionar por Conta da AWS e por região. Não é possível solicitar um aumento de cota.
Conjuntos de IPs confiáveis (lista de endereços IP)	1	O número máximo de listas de endereços IP confiáveis que podem ser carregadas e ativadas Conta da AWS por região. Não é possível solicitar um aumento de cota.
Listas de entidades de ameaças	6	O número máximo de listas de entidades de ameaças que você pode adicionar por Conta da AWS e por região. Não é possível solicitar um aumento de cota.

Recurso	Padrão	Comentários
Lista de entidades confiáveis	1	O número máximo de listas de entidades confiáveis que podem ser carregadas e ativadas Conta da AWS por região. Não é possível solicitar um aumento de cota.

GuardDuty Support para instâncias gerenciadas

A tabela a seguir indica o suporte que GuardDuty os vários recursos oferecem aos diferentes tipos de instâncias gerenciadas.

Tipo de recurso gerenciado	Suporte para monitoramento de tempo de execução	Proteção contra malware para suporte ao EC2
Modo automático do Amazon EKS	Compatível	Compatível
Instância AWS Fargate gerenciada do Amazon ECS	Sem suporte	Compatível
Instância gerenciada Lambda	Sem suporte	Sem suporte

Solução de problemas da Amazon GuardDuty

Quando você receber problemas relacionados à execução de uma ação específica GuardDuty, consulte os tópicos desta seção.

Tópicos

- Exportar as descobertas para o Amazon S3 - erro de acesso
- Proteção contra malware para problemas EC2
- Problemas de Runtime Monitoring
- Outros problemas de solução de problemas

Exportar as descobertas para o Amazon S3 - erro de acesso

Ao exportar GuardDuty descobertas para um bucket do Amazon S3 (destino de publicação), GuardDuty se não conseguir acessar esse destino de publicação, você poderá receber um erro de acesso.

Depois de definir as configurações para exportar descobertas, se não GuardDuty for possível exportar descobertas, ele exibirá uma mensagem de erro na página Configurações no GuardDuty console. Isso pode acontecer quando não GuardDuty consigo mais acessar o recurso de destino. Por exemplo, se o bucket do Amazon S3 foi excluído ou se a permissão para acessar o bucket foi modificada. Isso também pode acontecer quando GuardDuty você não consegue mais acessar a AWS KMS chave que foi usada para criptografar os dados em seu bucket do Amazon S3. Quando GuardDuty não consegue exportar, ele envia uma notificação para o e-mail associado à conta para fornecer informações sobre esse problema.

Como resolver o erro de acesso?

Para resolver o problema, certifique-se de que os recursos correspondentes existam e GuardDuty tenham as permissões para acessar os recursos necessários.

Para obter mais informações, consulte Exportar as descobertas geradas para bucket do Amazon S3.

O que acontece quando você não resolve esse erro?

Se você não resolver o problema antes que o período de retenção de descobertas de 90 dias termine GuardDuty, suas descobertas não serão exportadas. GuardDuty desativará a localização de configurações de exportação para essa conta na região específica.

Para começar a exportar as descobertas novamente, atualize as configurações na região específica.

Proteção contra malware para problemas EC2

Esta seção lista os erros que você pode enfrentar ao configurar ou usar a Proteção contra Malware para EC2.

Falta (obrigatório) AWS Organizations permissão de gerenciamento ao ativar a verificação de GuardDuty-initiated malware

Quando você deseja gerenciar várias contas usando AWS Organizations e recebe esse erroThe `request failed because you do not have the required AWS Organizations management account permission.`, você está perdendo a permissão para ativar a verificação de GuardDuty-initiated malware para várias contas em sua organização.

Para mais informações sobre como fornecer permissão à conta de gerenciamento, consulte Estabelecendo acesso confiável para permitir a verificação de GuardDuty-initiated malware.

Estou iniciando uma verificação de On-demand malware, mas isso resulta na falta de um erro de permissões necessárias.

Se você receber um erro sugerindo que você não tem as permissões necessárias para iniciar uma verificação de On-demand malware em uma instância do Amazon EC2, verifique se você anexou a AWS política gerenciada: AmazonGuardDutyFullAccess_v2 (recomendado) política à sua função do IAM.

Se você for membro de uma AWS organização e ainda receber o mesmo erro, conecte-se à sua conta de gerenciamento. Para obter mais informações, consulte AWS Organizations SCP — Acesso negado.

Eu recebo um GetRole erro **`iam:`** ao trabalhar com o Malware Protection for EC2.

Se você receber esse erro —`Unable to get role: AWSServiceRoleForAmazonGuardDutyMalwareProtection`, isso significa que você está perdendo a permissão para ativar a verificação de GuardDuty-initiated malware ou usar a verificação de On-demand malware. Verifique se você anexou a política AWS política gerenciada: AmazonGuardDutyFullAccess_v2 (recomendado) ao seu perfil do IAM.

Sou uma conta de GuardDuty administrador que precisa ativar a verificação de GuardDuty-initiated malware, mas não usa AWS política gerenciada: AmazonGuardDutyFullAccess para gerenciar GuardDuty.

- Configure a função do IAM que você usa GuardDuty para ter as permissões necessárias para ativar a verificação de GuardDuty-initiated malware. Para obter mais informações sobre as permissões necessárias, consulte Criação de uma função vinculada ao serviço para Proteção contra malware para EC2.
- Anexe AWS política gerenciada: AmazonGuardDutyFullAccess_v2 (recomendado) ao seu perfil do IAM. Isso ajudará você a ativar a verificação de GuardDuty-initiated malware nas contas dos membros.

Problemas de Runtime Monitoring

Esta seção lista os erros que você pode enfrentar ao configurar ou usar Runtime Monitoring.

Problemas de cobertura de runtime

Quando a cobertura de tempo de execução de seus recursos protegidos se torna insalubre, o GuardDuty console fornece o tipo exato de problema. Depois de definir o tipo de problema, use os documentos a seguir para ver as etapas de solução de problemas para cada tipo de recurso compatível:

- Solucionando problemas de cobertura de runtime do Amazon EC2
- Solução de problemas de cobertura ECS-Fargate de tempo de execução da Amazon
- Solucionando problemas de cobertura de runtime do Amazon EKS

Solução de problemas de falta de memória no Runtime Monitoring (somente suporte ao Amazon EC2)

Esta seção fornece as etapas de solução de problemas quando você enfrenta um erro de falta de memória com base na Limites de CPU e de memória implantação manual do agente de GuardDuty segurança.

Se `systemd` encerrar o GuardDuty agente por causa do `out-of-memory` problema e você avaliar que fornecer mais memória ao GuardDuty agente é razoável, você pode atualizar o limite.

1. Com a permissão do root, abra`/lib/systemd/system/amazon-guardduty-agent.service`.
2. Encontre `MemoryLimit` e `MemoryMax` e atualize os dois valores.

```
MemoryLimit=256M
MemoryMax=256M
```

3. Depois de atualizar os valores, reinicie o GuardDuty agente usando o seguinte comando:

```
sudo systemctl daemon-reload
sudo systemctl restart amazon-guardduty-agent
```

4. Execute o seguinte comando para visualizar o status:

```
sudo systemctl status amazon-guardduty-agent
```

   A saída esperada mostrará o novo limite de memória:

```
Main PID: 2540 (amazon-guardduty)
Tasks: 16
Memory: 21.9M (limit: 256.0M)
```

Meu AWS Step Functions o fluxo de trabalho está falhando inesperadamente

Se o GuardDuty contêiner contribuiu para a falha do fluxo de trabalho, consulteSolução de problemas de cobertura ECS-Fargate de tempo de execução da Amazon. Se o problema persistir, para evitar a falha do fluxo de trabalho devido ao GuardDuty contêiner, execute uma das seguintes etapas:

- Adicione a `false` tag`GuardDutyManaged`: ao cluster Amazon ECS associado.
- Desative a configuração automática do agente para AWS Fargate (somente ECS) no nível da conta. Adicione a tag de inclusão`GuardDutyManaged`: `true` ao cluster Amazon ECS associado que você deseja continuar monitorando com o agente GuardDuty automatizado.

Outros problemas de solução de problemas

Se você não encontrar um cenário adequado ao seu problema, veja as seguintes opções de solução de problemas:

- Para problemas gerais do IAM ao acessar o https://console.aws.amazon.com/guardduty/, consulteSolução de problemas de GuardDuty identidade e acesso da Amazon.
- Para problemas de autenticação e autorização durante o acesso AWS AWS Console Home, consulte Solução de problemas do IAM.

GuardDuty Regiões e endpoints da Amazon

Para ver Regiões da AWS onde a Amazon GuardDuty está disponível, consulte os GuardDuty endpoints da Amazon no Referência geral da Amazon Web Services.

Recomendamos que você ative GuardDuty em todos os compatíveis Regiões da AWS. Isso permite GuardDuty gerar descobertas sobre atividades não autorizadas ou incomuns, mesmo em regiões que você não está usando ativamente. Isso também permite GuardDuty monitorar AWS CloudTrail eventos para o suportado Regiões da AWS, reduzindo sua capacidade de detectar atividades que envolvam serviços globais.

Region-specific disponibilidade de recursos

Uma lista de diferenças regionais para especificar a disponibilidade dos GuardDuty recursos.

Campos filtráveis expandidos para CreateFilter e UpdateFilter

Os campos filtráveis adicionais para regras e filtros de supressão estão disponíveis somente na AWS partição ()`aws`. Em outras partições, você pode continuar usando os campos compatíveis com o console.

ListFindings e GetFindingsStatistics APIs

As APIs GetFindingsStatistics e ListFindings têm uma sinalização `consoleOnly` temporária. Ao usar qualquer uma dessas APIs ou ambas, a `consoleOnly` sinalização significa que a API é capaz de buscar resultados até um limite máximo de 1000.

Proteção contra malware para o EC2

GuardDuty suporta o Proteção contra malware para o EC2 recurso nas Zonas Locais AWS Dedicadas.

Proteção do RDS

A Proteção do RDS não tem suporte na região Ásia-Pacífico (Taipei) (`ap-east-2`).

A Proteção RDS não é suportada nas Zonas Locais AWS Dedicadas.

Tipo de descoberta do IAM — CredentialAccess:IAMUser/CompromisedCredentials

O tipo de CredentialAccess:IAMUser/CompromisedCredentials descoberta não é suportado nas seguintes regiões.

Região da AWS	Código da região
AWS GovCloud (US-West)	us-gov-west-1
AWS GovCloud (US-East)	us-gov-east-1
China (Pequim)	cn-north-1
China (Ningxia)	cn-northwest-1

Tipo de descoberta do IAM — DefenseEvasion:IAMUser/BedrockLoggingDisabled

O tipo de DefenseEvasion:IAMUser/BedrockLoggingDisabled descoberta não é suportado na região Ásia-Pacífico (Hong Kongap-east-1) ().

Tipos de descoberta do AI Protection

Os tipos de Impact:IAMUser/CostHarvesting descoberta Impact:IAMUser/AnomalousModelInvocation e de localização exigem Amazon Bedrock ou Amazon SageMaker AI. Regiões da AWS Onde o Amazon Bedrock não está disponível, GuardDuty gera esses tipos de descoberta somente a partir de invocações do modelo Amazon SageMaker AI. Para as regiões em que o Amazon Bedrock está disponível, consulte o Amazon Bedrock suportado Regiões da AWS no Guia do usuário do Amazon Bedrock.

O tipo de Impact:IAMUser/PromptInjection.Direct descoberta depende do Amazon Bedrock Guardrails, que não está disponível em todos. Regiões da AWS Esse tipo de descoberta é suportado somente nas regiões em que o Amazon Bedrock Guardrails está disponível. Para ver a lista atual, consulte Regiões suportadas para Amazon Bedrock Guardrails no Guia do usuário do Amazon Bedrock.

Suporte geral à API

As seguintes APIs na Amazon GuardDuty API Reference podem ter diferenças regionais devido à indisponibilidade de algumas das fontes de dados ou recursos especificados anteriormente: Regiões da AWS

- CreateDetector
- UpdateDetector
- UpdateMemberDetectors
- UpdateOrganizationConfiguration

- GetDetector
- GetMemberDetectors
- DescribeOrganizationConfiguration

Tipos de descoberta do Amazon EC2: DefenseEvasion:EC2/UnusualDoHActivity e DefenseEvasion:EC2/UnusualDoTActivity

A tabela a seguir mostra Regiões da AWS onde GuardDuty está disponível, mas esses dois tipos de descoberta do Amazon EC2 ainda não são suportados.

Região da AWS	Código da região
Ásia-Pacífico (Seul)	ap-northeast-2
Ásia-Pacífico (Osaka)	ap-northeast-3
Ásia-Pacífico (Jacarta)	ap-southeast-3

AWS GovCloud (US) Regiões

Para obter as informações mais recentes, consulte Amazon GuardDuty no Guia AWS GovCloud (US) do usuário.

Regiões da China

Para obter as informações mais recentes, consulte Disponibilidade de atributos e diferenças de implementação.

GuardDuty ações e parâmetros legados

GuardDuty A Amazon descontinuou algumas das ações e parâmetros da API, mas ainda os suporta. A prática recomendada é usar as novas ações e parâmetros da API que substituem as opções legadas. A tabela a seguir compara as ações e os parâmetros antigos e novos.

Legado actions/parameters	Novo actions/parameters	Comparação
DisassociateFromMasterAccount	DisassociateFromAdministratorAccount	Com a mesma implementação em ambas as ações, GuardDuty usa o termo `Administrator` em`DisassociateFromAdministratorAccount` .
`autoEnable` parâmetro em DescribeOrganizationConfiguratione UpdateOrganizationConfiguration	`autoEnableOrganizationMembers`	Com`autoEnableOrganizationMembers` , a conta GuardDuty do administrador pode auditar e aplicar GuardDuty qualquer um dos valores em todas as contas dos membros. Usando as APIs, pode levar até 24 horas para atualizar a configuração de todas as contas-membro. Para obter mais informações sobre os valores possíveis do `autoEnableOrganizationMembers` campo, consulte auto EnableOrganizationMembers
Parâmetro `dataSources` nas APIs listadas em GuardDuty Mudanças na API em março de 2023.	`features`	A partir de março de 2023, você pode configurar GuardDuty Proteção contra malware para EC2 e usar os novos planos de GuardDuty proteção`features`. Os planos de proteção lançados antes de março de 2023, incluindo a Proteção contra malware para o EC2, ainda oferecem

Legado actions/parameters	Novo actions/parameters	Comparação
		suporte à configuração que usa `dataSources` . Caso as APIs sejam usadas para configurar um plano de proteção, cada solicitação de API poderá incluir `dataSources` ou `features`, mas não ambos.

Histórico de documentos da Amazon GuardDuty

A tabela a seguir descreve mudanças importantes na documentação desde a última versão do Guia do GuardDuty usuário da Amazon. Para receber notificações sobre atualizações dessa documentação, é possível inscrever-se em um feed RSS.

Alteração	Descrição	Data
Novo recurso - Regras de detecção personalizadas para monitoramento de tempo de execução	As regras de detecção personalizadas GuardDuty agora oferecem suporte ao Runtime Monitoring para detectar atividades de hosts e contêineres, como escalonamento de privilégios, roubo de credenciais, comprometimento da defesa e fuga de contêineres no Amazon EKS, Amazon EC2 e Amazon ECS no Fargate. Para obter mais informações, consulte Regras de detecção personalizadas para monitoramento de tempo de execução. Essas regras também geram quatro novos tipos de descoberta do Runtime Monitoring. Para obter mais informações, consulte Tipos de localização que exigem regras de detecção personalizadas em Tipos de descoberta do GuardDuty Runtime Monitoring.	15 de outubro de 2026

Tipo de descoberta atualizado - UnauthorizedAccess:IAMUser/ResourceCredentialExfiltration.InsideAWS	A ResourceCredentialExfiltration.InsideAWS descoberta atual agora detecta a exfiltração de credenciais do Lambda, além do Amazon ECS. Para obter mais informações, consulte UnauthorizedAccess:IAMUser/ResourceCredentialExfiltration.InsideAWS.	28 de setembro de 2026
Funcionalidade atualizada – Monitoramento de Runtime	GuardDuty O Runtime Monitoring lança a nova versão 1.17.1 do agente de segurança para recursos do Amazon EKS, Amazon EC2 e Amazon ECS.AWS Fargate Para obter mais informações sobre a nova versão do agente e uma lista de recursos adicionais para atualizar seu agente de segurança, consulte Versões de lançamento do agente de GuardDuty segurança.	18 de setembro de 2026

Documentação atualizada - Plataformas suportadas pelo Runtime Monitoring	GuardDuty O Runtime Monitoring adicionou uma página consolidada de arquiteturas de CPU, sistemas operacionais e versões do kernel compatíveis. As páginas de pré-requisitos para instâncias do Amazon EC2 (somente Amazon ECS) e clusters do AWS Fargate Amazon EKS agora fazem referência a esta página para as arquiteturas de CPU, distribuições de sistema operacional e versões de kernel verificadas. Esta página agora inclui a versão 6.18 do kernel Bottlerocket.	18 de setembro de 2026
Campos de AWS CloudTrail eventos editados documentados para regras de detecção personalizadas	Foi adicionada uma orientação explicando que um AWS serviço pode redigir o valor de um campo nos AWS CloudTrail eventos que ele publica e que uma regra de detecção personalizada cuja lógica de detecção depende de um campo redigido não corresponde. Para obter mais informações, consulte Campos de eventos redigidos.	18 de setembro de 2026

A proteção de IA contribui para a detecção da sequência de ataque	GuardDuty A Detecção Estendida de Ameaças agora inclui as descobertas da Proteção de GuardDuty IA entre os sinais que ela correlaciona para detectar uma sequência de ataque. Para obter mais informações, consulte Detecção GuardDuty estendida de ameaças e proteção de GuardDuty IA.	17 de setembro de 2026
Função GuardDuty vinculada ao serviço (SLR) atualizada	GuardDuty atualizou a função vinculada ao serviço (SLR) para incluir as permissões e. `vpc-lattice:CreateServiceNetworkVpcAssociation` `vpc-lattice:AssociateViaAWSService` Essas permissões permitem GuardDuty usar as ações do Amazon VPC Lattice para habilitar a conectividade do agente Runtime Monitoring. Para obter mais informações, consulte permissões de Service-linked função para GuardDuty.	9 de setembro de 2026

Novo recurso - Regras de detecção personalizadas	GuardDuty apresenta as Regras de Detecção Personalizadas, uma biblioteca organizada de regras de detecção alinhadas às técnicas dos agentes de ameaças. Você pode procurar, ativar e gerenciar regras para detectar técnicas específicas em seu ambiente. Para obter mais informações, consulte Regras de detecção personalizadas.	1 de setembro de 2026
Funcionalidade atualizada — GuardDuty Investigação (pré-visualização)	Removido o limite de 100 contas para investigações em nível organizacional. As investigações da organização agora analisam todas as contas em sua organização. Para obter mais informações, consulte GuardDutyInvestigação.	24 de agosto de 2026

Funcionalidade atualizada – Monitoramento de Runtime	GuardDuty O Runtime Monitoring lança a nova versão 1.16.0 do agente de segurança para recursos do Amazon EKS, Amazon EC2 e Amazon ECS.AWS Fargate Para obter mais informaçõ es sobre a nova versão do agente e uma lista de recursos adicionais para atualizar seu agente de segurança, consulte Versões de lançamento do agente de GuardDuty segurança.	17 de julho de 2026
Novo tipo de descoberta - UnauthorizedAccess:IAMUser/ ResourceCredentialExfiltrat ion.InsideAWS e tipo de descoberta atualizado - UnauthorizedAccess:IAMUser/ ResourceCredentialExfiltrat ion.OutsideAWS	GuardDuty introduz um novo tipo de descoberta que detecta quando AWS credenciais temporárias criadas para uma tarefa do Amazon ECS são usadas de outra. Conta da AWS Além disso, a ResourceCredentialExfiltrat ion.OutsideAWS descobert a existente agora detecta a exfiltração de credencia is de tarefas do Amazon ECS, além do Lambda. Para obter mais informações, consulte UnauthorizedAccess :IAMUser/ResourceCredential Exfiltration.InsideAWS e UnauthorizedAccess:IAMUser/ ResourceCredentialExfiltrat ion.OutsideAWS.	15 de julho de 2026

Novo plano de proteção - GuardDuty AI Protection	GuardDuty O AI Protection detecta ameaças às cargas de trabalho de IA que usam o Amazon Bedrock e o Amazon AI. SageMaker Quando você ativa o AI Protection, GuardDuty analisa os eventos de AWS CloudTrail dados desses serviços para detectar invocações anômalas de modelos, ataques de coleta de custos e tentativas diretas de injeção imediata. Para obter mais informações, consulte Proteção de GuardDuty IA.	13 de julho de 2026
Detalhes adicionais sobre ameaças no esquema de EventBridge eventos da Amazon para o Malware Protection for S3	O resultado do escaneamento de objetos do Malware Protection for S3, o EventBridge evento Amazon agora fornece detalhes adicionais sobre ameaças. Os novos campos incluem `source` `itemDetails hash`,, `itemPath` e. Para obter mais informações, consulte Resultado da digitalização de objetos do S3.	7 de julho de 2026

GuardDuty Investigação (prévia)	A Amazon GuardDuty agora oferece AI-powered investigações em pré-visualização pública. Você pode criar investigações para analisar automaticamente GuardDuty descobertas e contas e receber um resumo estruturado em minutos com disposição com pontuação de confiança, classificação técnica MITRE ATT&CK® e recomendações práticas. Você pode iniciar investigações a partir do GuardDuty console, da CLI, da API AWS ou do servidor MCP. O Preview está disponível em 10 Regiões da AWS: Leste dos EUA (Norte da Virgínia), Leste dos EUA (Ohio), Oeste dos EUA (Oregon), Canadá (Central), Europa (Frankfurt), Europa (Irlanda), Europa (Londres), Europa (Paris), Europa (Estocolmo) e Ásia-Pacífico (Tóquio). Para obter mais informações, consulte GuardDutyInvestigação.	22 de junho de 2026
Amazon RDS para MariaDB e MySQL	O Database Insights já está disponível.	11 de junho de 2026

Atualização da funcionalidade - Proteção contra Malware para S3	GuardDuty aumentou as cotas do Malware Protection for S3 para o número máximo de arquivos que podem ser extraídos e analisados de um arquivamento e os níveis máximos de arquivos aninhados que podem ser extraídos. Para obter mais informações, consulte Cotas na Proteção contra malware para o S3.	9 de junho de 2026
Novos tipos de descoberta do Runtime Monitoring - Sensitive FileModified	GuardDuty O Runtime Monitoring apresenta três novos tipos de descoberta que informam quando um arquivo de sistema sensível à segurança em uma instância ou contêiner do Amazon EC2 foi modificado, potencialmente permitindo que um adversári o ganhe persistência, eleve privilégios ou evite a detecção. Para obter mais informações, consulte Persistence:Runtim e/SensitiveFileModified, PrivilegeEscalation:Runtime /SensitiveFileModified e DefenseEvasion:Runtime/ SensitiveFileModified.	2 de junho de 2026

Funcionalidade atualizada - Encontrando critérios de filtro	Os campos não compatíveis foram removidos da lista de critérios do filtro de localização. Para obter mais informações, consulte Filtrando descobertas em GuardDuty.	29 de maio de 2026
Dois tipos de descoberta retirados	Os tipos de Persistence:Kubernetes/ContainerWithSensitiveMountdescoberta PrivilegeEscalation:Kubernetes/PrivilegedContainere foram retirados.	29 de maio de 2026
Funcionalidade atualizada – Monitoramento de Runtime	GuardDuty Monitoramento de tempo de execução Foi adicionado suporte para o Kubernetes versão 1.36. Para obter mais informações, consulte Pré-requisitos para monitoramento de tempo de execução.	28 de maio de 2026
Funcionalidade atualizada – Monitoramento de Runtime	GuardDuty O Runtime Monitoring lança a nova versão 1.15.0 do agente de segurança para recursos do Amazon ECS.AWS Fargate Para obter mais informações sobre a nova versão do agente e uma lista de recursos adicionais para atualizar seu agente de segurança, consulte Versões de lançamento do agente de GuardDuty segurança.	28 de maio de 2026

Funcionalidade atualizada – Detecção de Ameaças Avançada	GuardDuty O Extended Threat Detection adiciona cinco novos tipos de indicadores à sequência de ataque, encontrando detalhes: MALICIOUS_PACKAGE, MISCONFIGURATION, REACHABILITY, SENSITIVE_DATA e VULNERABILITY. Para obter mais informações, consulte Detalhes da descoberta da sequência de ataque.	20 de maio de 2026
Funcionalidade atualizada – Monitoramento de Runtime	GuardDuty O Runtime Monitoring lança a nova versão 1.15.0 do agente de segurança para recursos do Amazon EKS e do Amazon EC2. Para obter mais informações sobre a nova versão do agente e uma lista de recursos adicionais para atualizar seu agente de segurança, consulte Versões de lançamento do agente de GuardDuty segurança.	14 de maio de 2026

Atualizado AmazonGuardDutyServiceRolePolicy	Adicionou `s3:ListBucket` , `ecs:DescribeTasks` , e `ecs:DescribeTaskDefinition` permissões à função GuardDuty vinculada ao serviço. Para obter mais informações, consulte GuardDutyatualizações nas políticas AWS gerenciadas.	23 de abril de 2026
Funcionalidade atualizada – Monitoramento de Runtime	GuardDuty O Runtime Monitoring lança a nova versão 1.12.2 do agente de segurança para recursos do Amazon EKS. Para obter mais informações sobre a nova versão do agente e uma lista de recursos adicionais para atualizar seu agente de segurança, consulte Versões de lançamento do agente de GuardDuty segurança.	22 de abril de 2026
Funcionalidade atualizada - Campos filtráveis expandidos	GuardDuty agora oferece suporte à filtragem em qualquer campo de busca ao criar ou atualizar regras de supressão. Os campos de carimbo de data/hora aceitam valores no formato de milissegundos do Unix Epoch. Para obter mais informações, consulte Filtrando descobertas em GuardDuty.	20 de abril de 2026

Atualização da funcionalidade - Proteção contra Malware para S3	A EventBridge notificação dos resultados do escaneamento de objetos do S3 agora inclui um `statusReasons` campo `scanResultDetails` quando um escaneamento é ignorado. Esse campo fornece o motivo específico pelo qual o escaneamento foi ignorado. Para obter mais informações, consulte Status de verificação potencial do objeto S3 e status do resultado.	10 de abril de 2026
Funcionalidade atualizada – Monitoramento de Runtime	GuardDuty O Runtime Monitoring lança a nova versão 1.9.2 do agente de segurança para recursos do Amazon EC2. Para obter mais informações sobre novas versões do agente e uma lista de recursos adicionais para atualizar seu agente de segurança, consulte Versões de lançamento do agente de GuardDuty segurança.	3 de abril de 2026
Atualizado AmazonGuardDutyServiceRolePolicy	Foi adicionada a `cloudtrail:CreateServiceLinkedChannel` permissão para ativar um mecanismo adicional para consumir AWS CloudTrail eventos. Para obter mais informações, consulte GuardDuty atualizações nas políticas AWS gerenciadas.	25 de março de 2026

Funcionalidade atualizada – Monitoramento de Runtime	GuardDuty Monitoramento de tempo de execução Foi adicionado suporte para o Kubernetes versão 1.35. Para obter mais informações, consulte Pré-requisitos para monitoramento de tempo de execução.	20 de março de 2026
Nova política de acesso total `AmazonGuardDutyFullAccess_v2` com escopo reduzido substitui `AmazonGuardDutyFullAccess` .	A partir de 13 de março de 2026, a política GuardDuty foi descontinuada e a substitui u por uma `AmazonGuardDutyFullAccess` política com escopo reduzido chamada. `AmazonGuardDutyFullAccess_v2` Para obter mais informaçõ es, consulte política AWS gerenciada: AmazonGuardDutyFullAccess _v2.	13 de março de 2026
Novo tipo de descoberta – CredentialAccess:IAMUser/CompromisedCredentials	GuardDuty Apresenta um novo tipo de descoberta que detecta quando uma chave de acesso do IAM considera da potencialmente comprometida é usada para invocar operações de API em. AWS Para obter mais informações, consulte CredentialAccess:IAMUser/CompromisedCredentials.	6 de março de 2026

Novo tipo de descoberta – UnauthorizedAccess:IAMUser/ResourceCredentialExfiltration.OutsideAWS	GuardDuty introduz um novo tipo de descoberta que detecta quando um host externo AWS tenta executar operações de AWS API usando AWS credenciais temporárias criadas em um AWS Lambda recurso em seu ambiente. AWS Para obter mais informações, consulte UnauthorizedAccess:IAMUser/ResourceCredentialExfiltration.OutsideAWS.	16 de dezembro de 2025
Funcionalidade atualizada – Monitoramento de Runtime	GuardDuty O Runtime Monitoring lança a nova versão 1.9.1 do agente de segurança para recursos do Amazon EC2. Para obter mais informações sobre novas versões do agente e uma lista de recursos adicionais para atualizar seu agente de segurança, consulte Versões de lançamento do agente de GuardDuty segurança.	2 de dezembro de 2025

Funcionalidade atualizada – Monitoramento de Runtime	GuardDuty O Runtime Monitoring lança a nova versão 1.12.1 do agente de segurança para recursos do Amazon EKS. Para obter mais informações sobre a nova versão do agente e uma lista de recursos adicionais para atualizar seu agente de segurança, consulte Versões de lançamento do agente de GuardDuty segurança.	2 de dezembro de 2025
Funcionalidade atualizada – Detecção de Ameaças Avançada	GuardDuty O Extended Threat Detection introduz dois novos tipos de descoberta de sequências de ataque que ajudam a detectar ataques em vários estágios envolvendo instâncias comprometidas do Amazon EC2 e clusters do Amazon ECS. AttackSequence:EC2/CompromisedInstanceGroup AttackSequence:ECS/CompromisedCluster Ative o Runtime Monitoring para maximizar a detecção de ameaças. Para obter mais informações, consulte Tipos de descoberta de sequências de ataque.	2 de dezembro de 2025

Novo recurso - Curingas nas regras de supressão	GuardDuty aprimorou seus recursos de supressão com a introdução de partidas e NotMatches condições que oferecem suporte a curingas. Agora, os clientes podem usar * (para corresponder a qualquer número de caractere s) e? (para combinar no máximo 1 caractere) como curingas ao criar regras de supressão. Regras de supressão.	2 de dezembro de 2025
Novo recurso - Amazon CloudWatch Usage Metrics Support	GuardDuty introduz a publicação de métricas de uso na Amazon CloudWatch para todos os planos de proteção, permitindo que os clientes monitorem o uso. Para obter mais informações, consulte Monitoramento GuardDuty do uso e estimativa de custos	25 de novembro de 2025
Novo tipo de descoberta – DefenseEvasion:IAMUser/BedrockLoggingDisabled	GuardDuty apresenta um novo tipo de descoberta que detecta quando o registro de invocação do modelo Amazon Bedrock está desativado, o que pode indicar tentativas de evitar a detecção da atividade da carga de trabalho de IA. Para obter mais informações, consulte DefenseEvasion:IAMUser/BedrockLoggingDisabled .	21 de novembro de 2025

Novo recurso - Proteção contra malware para backup	GuardDuty A Proteção contra Malware para Backup agora está disponível em todas as regiões comerciais em GuardDuty que está disponível. Esse recurso ajuda você a detectar a possível presença de malware em seus recursos de backup por meio de varreduras completas e incrementais de snapshots, AMIs do EC2 e pontos de recuperação do Amazon EBS. Para obter mais informações sobre esse recurso, consulte Proteção contra malware para backup	19 de novembro de 2025
Alterar para AmazonGuardDutyFullAccess e AmazonGuardDutyFullAccess_V2	Permissão adicionada que permite passar uma função do IAM para GuardDuty quando você ativa a Proteção contra Malware para Backup.	19 de novembro de 2025
Novo recurso - Proteção contra malware para escaneamento sob demanda do S3.	GuardDuty anuncia o Scan on Demand for Malware Protection para S3. Usando esse recurso, você pode usar a nova SendObjectMalwareScan API para acionar escaneamentos em qualquer objeto já existente armazenado em seus buckets do S3. Para obter informações, consulte Escaneamento de malware S3 sob demanda.	17 de novembro de 2025

Funcionalidade atualizada – Monitoramento de Runtime	GuardDuty O Runtime Monitoring lança a nova versão 1.9.0 do agente de segurança para recursos do Amazon ECS.AWS Fargate Para obter informações sobre novas versões do agente e uma lista de recursos adicionais para atualizar seu agente de segurança, consulte Versões de lançamento do agente de GuardDuty segurança.	28 de outubro de 2025
Funcionalidade atualizada – Monitoramento de Runtime	GuardDuty O Runtime Monitoring lança a nova versão 1.9.0 do agente de segurança para recursos do Amazon EC2. Para obter informações sobre novas versões do agente e uma lista de recursos adicionais para atualizar seu agente de segurança, consulte Versões de lançamento do agente de GuardDuty segurança.	23 de outubro de 2025

Novo tipo de descoberta do Monitoramento de Runtime – DefenseEvasion:Runtime/KernelModuleLoaded	GuardDuty O Runtime Monitoring apresenta um novo tipo de descoberta que ajuda a identificar técnicas de evasão de defesa em que os agentes de ameaças usam módulos do kernel para contornar os controles de segurança, modificar as operações do sistema e obter acesso persistente ao sistema. Para obter mais informações, consulte DefenseEvasion:Runtime/KernelModuleLoaded.	15 de outubro de 2025
Funcionalidade atualizada – Monitoramento de Runtime	Foi adicionado suporte ao Kubernetes versão 1.34 para as distribuições do sistema operacional e à versão do agente de segurança para recursos do Role GuardDuty SageMaker Manager para Amazon EKS. Para obter mais informações, consulte Validar requisitos de arquitetura para o Amazon EKS.	3 de outubro de 2025

Orientação de solução de problemas de banco de dados do Amazon RDS adicionada	Diretrizes adicionadas para resolver problemas de banco de dados do RDS que podem afetar os recursos de monitoramento do GuardDuty RDS Protection, incluindo `storage-full` status e requisitos de réplica de leitura do RDS para PostgreSQL. Para obter mais informações, consulte Solucionar problemas de monitoramento da Proteção do RDS.	15 de setembro de 2025
Funcionalidade atualizada – Monitoramento de Runtime	Foi adicionada a distribuição Ubuntu Noble OS com suporte para as versões 6.13 e 6.14 do kernel para GuardDuty Runtime Monitoring para Amazon EC2. Para obter informações sobre a versão do agente EC2 compatível com essa distribuição de sistema operacional, consulte Validar requisitos de arquitetura para o Amazon EC2.	13 de setembro de 2025
Funcionalidade atualizada – Proteção do RDS	Foi adicionado suporte ao PostgreSQL 17 para RDS para bancos de dados PostgreSQL monitorados pelo RDS Protection. GuardDuty Para obter mais informações, consulte Bancos de dados compatíveis na Proteção do RDS.	13 de setembro de 2025

Atualização da funcionalidade - Proteção contra Malware para S3	GuardDuty O Malware Protection for S3 aumenta a cota padrão dos arquivos de arquivamento extraídos de 1.000 para 10.000 arquivos. Para obter mais informações, consulte Cotas na Proteção contra malware para o S3.	3 de setembro de 2025
Funcionalidade atualizada – Monitoramento de Runtime	GuardDuty O Runtime Monitoring lança a nova versão 1.11 do agente de segurança para recursos do Amazon EKS. Para obter mais informações sobre a nova versão do agente e uma lista de recursos adicionais para atualizar seu agente de segurança, consulte Versões de lançamento do agente de GuardDuty segurança.	29 de agosto de 2025

Funcionalidade atualizada – trabalho com listas	GuardDuty apresenta listas personalizadas de entidades confiáveis e de ameaças que oferecem suporte a endereços IP e nomes de domínio. GuardDuty continua oferecend o suporte à lista de endereços IP e recomenda o uso da lista de entidades para detecção personalizada de ameaças. Para mais informações, consulte Personalização de detecção de ameaças com listas de entidade e de endereços IP.	15 de agosto de 2025
Funcionalidade atualizada – Monitoramento de Runtime	GuardDuty O Runtime Monitoring lança a nova versão 1.8.0 do agente de segurança para os recursos do Amazon EC2 e do Amazon AWS Fargate ECS. Para obter mais informações sobre novas versões do agente e uma lista de recursos adicionais para atualizar seu agente de segurança, consulte Versões de lançamento do agente de GuardDuty segurança.	12 de agosto de 2025

Suporte para a região Ásia-Pacífico (Taipei)	A Amazon agora GuardDuty está disponível na região Ásia-Pacífico (Taipei) (`ap-east-2`). Para habilitar GuardDuty nessa região, consulte Introdução. Você pode receber notificações sobre atualizações dos GuardDuty recursos e detecções de ameaças assinando os anúncios do Amazon GuardDuty SNS nesta região.	31 de julho de 2025
Atualização da funcionalidade - Proteção contra Malware para S3	A Proteção contra malware para S3 agora oferece suporte para a verificação de objetos de até 100 GB, aumentado de 5 GB. Isso inclui objetos individuais e arquivamentos extraídos. Para obter mais informações, consulte Cotas na Proteção contra malware para o S3.	23 de julho de 2025

Funcionalidade atualizada – foi adicionado o proprietário esperado do bucket nas listas de IP confiável e de ameaças	GuardDuty adicionou o campo Proprietário esperado do bucket para listas de IPs confiáveis e IPs de ameaças. Nesse campo opcional, você pode especificar uma Conta da AWS ID que GuardDuty será usada para verificar a propriedade do bucket do Amazon S3. Para ter mais informações, consulte Working with trusted IP lists and threat lists.	16 de julho de 2025

Funcionalidade atualizada – Detecção de Ameaças Avançada	GuardDuty O Extended Threat Detection agora expande o suporte para clusters do Amazon EKS correlacionando vários sinais de segurança nos registros de auditoria do EKS, no comportamento dos processos em tempo de execução e na atividade da AWS API. Habilite a Proteção do EKS, o Monitoramento de Runtime (com o complemento do EKS) ou ambos para maximizar a detecção de ameaças. Para identificar ameaças potenciais, GuardDuty introduz um novo tipo de descoberta — AttackSequence:EKS/CompromisedCluster. Para obter mais informações, consulte Detecção de Ameaças Avançada.	17 de junho de 2025

Atualização da funcionalidade - Proteção contra Malware para S3	A Proteção contra malware para S3 não oferece suporte à verificação de arquivamentos com taxa de compactação extremamente alta. Esses arquivos serão ignorados durante a verificação e marcados com o resultado de verificação `UNSUPPORTED` . Para obter mais informações, consulte Status de verificação potencial do objeto S3 e status do resultado.	13 de junho de 2025
Funcionalidade atualizada – Proteção contra Malware para EC2	A Proteção contra malware para EC2 adicionou suporte para verificar a maioria das instâncias com `productCode` como `marketplace` . Isso se aplica tanto à verificação de GuardDuty-initiated malware quanto à verificação de On-demand malware. Para obter mais informações, consulte Razões para ignorar o recurso durante a verificação de malware.	13 de junho de 2025

Nova política AmazonGuardDutyFullAccess _v2	Foi adicionada uma nova AmazonGuardDutyFullAccess_v2 política com permissões para aprimorar a segurança restringindo as ações administrativas aos diretores GuardDuty de serviços. Para obter informações sobre essa política recomendada, consulte a política gerenciada pela AWS : AmazonGuardDutyFullAccess_v2.	4 de junho de 2025
Suporte regional expandido para proteção do RDS	GuardDuty O RDS Protection agora está disponível nas regiões do México (Central), Ásia-Pacífico (Tailândia) e Ásia-Pacífico (Malásia). A Proteção do RDS ajuda você a detectar comportamentos de login potencialmente suspeitos nos sistemas compatíveis Aurora MySQL, Aurora PostgreSQL (incluindo Limitless Database) e RDS for PostgreSQL. No caso de detecção de ameaças, GuardDuty gera uma descoberta de proteção do RDS. Para obter mais informações sobre bancos de dados compatíveis e habilitar esse plano de proteção nas regiões recém-compatíveis, consulte Proteção do RDS.	4 de junho de 2025

Funcionalidade atualizada – Monitoramento de Runtime	GuardDuty O Runtime Monitoring lança a nova versão 1.7.1 do agente de segurança para recursos do Amazon EC2. Para obter mais informações sobre novas versões do agente e uma lista de recursos adicionais para atualizar seu agente de segurança, consulte Versões de lançamento do agente de GuardDuty segurança.	3 de junho de 2025
Suporte para Detecção de Ameaças Avançada	GuardDuty A Detecção Estendida de Ameaças agora está disponível na Ásia-Pacífico (Tailândia) (ap-southeast-7). Sem a necessidade de ativação, ele detecta ataques em vários estágios que abrangem fontes de dados, vários tipos de AWS recursos e tempo, dentro de um. Conta da AWS Quando ameaças potenciais são detectada s, ela gera uma descobert a da sequência de ataque. Para obter mais informaçõ es, consulte Detecção de Ameaças Avançada.	12 de maio de 2025

Suporte para a região México (Centro)	A Amazon agora GuardDuty está disponível na região do México (Central) `mx-central-1` (). Para habilitar GuardDuty nessa região, consulte Introdução. Você pode receber notificaç ões sobre atualizações dos GuardDuty recursos e detecções de ameaças assinando os anúncios do Amazon GuardDuty SNS nesta região.	7 de maio de 2025
Funcionalidade atualizada – Monitoramento de Runtime	GuardDuty O Runtime Monitoring lança a nova versão 1.10.0 do agente de segurança para recursos do Amazon EKS. Para obter mais informações sobre novas versões do agente e uma lista de recursos adicionais para atualizar seu agente de segurança, consulte Versões de lançamento do agente de GuardDuty segurança.	04 de abril de 2025

Funcionalidade atualizada – Monitoramento de Runtime	GuardDuty O Runtime Monitoring lança a nova versão 1.7.0 do agente de segurança para recursos da Amazon ECS-Fargate. Para obter mais informações sobre novas versões do agente e uma lista de recursos adicionais para atualizar seu agente de segurança, consulte Versões de lançamento do agente de GuardDuty segurança.	04 de abril de 2025
Funcionalidade atualizada – Monitoramento de Runtime	GuardDuty O Runtime Monitoring lança a nova versão 1.7.0 do agente de segurança para recursos do Amazon EC2. Para obter mais informações sobre novas versões do agente e uma lista de recursos adicionais para atualizar seu agente de segurança, consulte Versões de lançamento do agente de GuardDuty segurança.	3 de abril de 2025

Suporte para a região Ásia-Pacífico (Tailândia)	A Amazon agora GuardDuty está disponível na região Ásia-Pacífico (Tailândia). Para obter informações sobre quais recursos são compatíveis nesta região, consulte disponibilidade de Region-specific recursos. Para habilitar GuardDuty nessa região, consulte Introdução. Você pode receber notificaç ões sobre atualizações dos GuardDuty recursos e detecções de ameaças assinando os anúncios do Amazon GuardDuty SNS.	1.º de abril de 2025
Funcionalidade atualizada	O painel de resumo agora mostra insights com base em todas as descobertas de segurança geradas, removendo a restrição anterior de 5.000 descobertas. Para obter informações sobre esses insights, consulte Painel de GuardDuty resumo.	17 de março de 2025

Funcionalidade atualizada – Monitoramento de Runtime	GuardDuty O Runtime Monitoring lança a nova versão 1.9.0 do agente de segurança para recursos do Amazon EKS. Para obter mais informações sobre novas versões do agente e uma lista de recursos adicionais para atualizar seu agente de segurança, consulte Versões de lançamento do agente de GuardDuty segurança.	2 de março de 2025
Funcionalidade atualizada – Monitoramento de Runtime	GuardDuty O Runtime Monitoring adicionou um novo tipo de problema de cobertura (Agente não provisionado) para recursos do Amazon EC2. Para obter informaçõ es sobre a solução desse problema, consulte Solução de problemas de cobertura de runtime do Amazon EC2.	21 de fevereiro de 2025

Funcionalidade atualizada – Monitoramento de Runtime	GuardDuty O Runtime Monitoring lança novos agentes de segurança para recursos do Amazon EC2 e da Amazon ECS-Fargate . Para obter mais informaçõ es sobre novas versões do agente e uma lista de recursos adicionais para atualizar seus agentes de segurança, consulte Versões de lançamento do agente de GuardDuty segurança.	6 de fevereiro de 2025
GuardDuty suporte na região existente da Ásia-Pacífico (Malásia)	GuardDuty A Detecção Estendida de Ameaças agora está disponível na região Ásia-Pacífico (Malásia). Para obter mais informaçõ es, consulte Detecção de Ameaças Avançada.	28 de janeiro de 2025

Suporte para a região da Ásia-Pacífico (Malásia)	A Amazon agora GuardDuty está disponível na região Ásia-Pacífico (Malásia) . Para obter informações sobre quais recursos são compatíveis nesta região, consulte disponibilidade de Region-specific recursos. Para habilitar GuardDuty nessa região, consulte Introdução. Você pode receber notificaçõ es sobre atualizações dos GuardDuty recursos e detecções de ameaças assinando os anúncios do Amazon GuardDuty SNS.	16 de janeiro de 2025
Funcionalidade atualizada – Monitoramento de Runtime	GuardDuty O Runtime Monitoring atualizou informaçõ es adicionais e etapas de solução de problemas de ECS-Fargate cobertura da Amazon associados ao agente não provisionado. Para obter mais informações sobre o tipo de problema do Agente não provisionado, consulte Solução de problemas de cobertura de ECS-Farga te tempo de execução da Amazon.	8 de janeiro de 2025

Novo tipo de descoberta – Policy:IAMUser/ShortTermRootCredentialUsage	GuardDuty introduz um novo tipo de descoberta que alerta você quando credenciais de usuário restritas, criadas para os listados Contas da AWS em seu ambiente, estão sendo usadas para fazer solicitações para. Serviços da AWS Para obter mais informações, consulte Policy:IAMUser/ShortTermRootCredentialUsage.	8 de janeiro de 2025
Novo recurso - Detecção GuardDuty estendida de ameaças	GuardDuty anuncia a Detecção Estendida de Ameaças para detectar sequências de ataque em vários estágios que abrangem fontes de dados e AWS recursos GuardDuty fundamentais em você Conta da AWS, durante um período específico. Sem custo adicional, esse recurso é ativado automaticamente para todas as contas que foram ativadas GuardDuty . Esse recurso anuncia dois novos tipos de GuardDuty descoberta, chamados de tipos de descoberta de sequência de ataque. Para obter mais informações, consulte Detecção de Ameaças Avançada.	1.º de dezembro de 2024

Funcionalidade aprimorada entre serviços – Monitoramento de Runtime e Proteção contra malware para EC2	Impacto dos novos recursos do Amazon Elastic Kubernetes Service (Amazon EKS) nos recursos da Amazon: GuardDuty • Modo automático do Amazon EKS – tanto o Monitoramento de Runtime para o Amazon EKS quanto a Proteção contra malware para EC2 oferecem suporte a isso. • Amazon EKS Hybrid Nodes – tanto o Monitoramento de Runtime para o Amazon EKS quanto a Proteção contra malware para EC2 não oferecem suporte a isso. Para obter mais informações, consulte Como o Monitoramento de Runtime funciona com clusters do Amazon EKS e a Proteção contra Malware para EC2.	1.º de dezembro de 2024

Funcionalidade atualizada no Runtime Monitoring - Amazon EKS	O Monitoramento de Runtime lançou uma nova versão do agente 1.8.1 (v1.8.1-eks-build.2) para recursos do Amazon EKS. Com essa nova versão do agente, GuardDuty amplia o suporte do Runtime Monitoring para recursos do Amazon EKS que são executados no RedHat CentOS e no Fedora. Para obter mais informações, consulte Validar os requisitos de arquitetura. Para obter informações sobre as notas de lançamento, consulte Agente GuardDuty de segurança para recursos do Amazon EKS.	23 de novembro de 2024
Funcionalidade atualizada no Runtime Monitoring - Amazon EC2	O Runtime Monitoring lançou uma nova versão 1.5.0 do agente para recursos do Amazon EC2. Com essa nova versão do agente, GuardDuty amplia o suporte do Runtime Monitoring para recursos do Amazon EC2 que são executados no RedHat CentOS e no Fedora. Para obter mais informações, consulte Validar os requisitos de arquitetura. Para obter informações sobre as notas de lançamento, consulte Agente GuardDuty de segurança para recursos do Amazon EC2.	20 de novembro de 2024

Funcionalidade atualizada no monitoramento de tempo de execução - Amazon ECS-Fargate	O Runtime Monitoring lançou uma nova versão 1.5.0 do agente para ECS-Fargate recursos da Amazon. Para obter mais informações sobre as notas de lançamento, consulte o agente de GuardDuty segurança para AWS Fargate (somente Amazon ECS).	14 de novembro de 2024
Atualização da funcionalidade na Proteção contra Malware para EC2	GuardDuty O Malware Protection for EC2 adicionou três tipos de descoberta do Runtime Monitoring à lista de descobertas que invocam a verificação de GuardDuty-initiated malware nas instâncias do Amazon EC2. As contas que habilitaram a Proteção contra Malware para EC2 observarão a verificação de GuardDuty-initiated malware ao GuardDuty gerar qualquer uma das seguintes descobertas: • Execution:Runtime/MaliciousFileExecuted • Execution:Runtime/SuspiciousShellCreated • PrivilegeEscalation:Runtime/ElevationToRoot	7 de novembro de 2024

Atualização da funcionalidade na Proteção do RDS	GuardDuty O RDS Protection adiciona a versão recém-lançada do `16.4-limitless` mecanismo de banco de dados Aurora PostgreSQL Limitless à lista de bancos de dados compatíveis. Por Contas da AWS isso, já habilitou o RDS Protection, GuardDuty iniciará automaticamente o monitoramento do comportamento de login para o banco de dados Limitless. As contas que já consumiram o teste gratuito de 30 dias a Proteção do RDS incorrerão no custo de uso associado ao Limitless Database, junto com outros bancos de dados compatíveis que são monitorados. Para obter mais informações, consulte Proteção RDS.	6 de novembro de 2024

Expansão GuardDuty e AWS PrivateLink integração da região	GuardDuty agora estende o suporte regional para a Amazon GuardDuty e os endpoints de interface VPC ().AWS PrivateLink Anteriormente, o suporte regional estava disponível para Leste dos EUA (Norte da Virgínia), Europa (Irlanda) e Israel (Tel Aviv). Esse suporte agora está estendido a todos os Regiões da AWS lugares GuardDuty disponíveis. Para obter mais informações sobre diferenças regionais, consulte disponibilidade de Region-specific recursos.	6 de novembro de 2024
Funcionalidade atualizada no monitoramento de tempo de execução - Amazon ECS-Fargate	O Runtime Monitoring lançou uma nova versão 1.4.1 do agente para ECS-Fargate recursos da Amazon. Para obter mais informações sobre as notas de lançamento, consulte o agente de GuardDuty segurança para AWS Fargate (somente Amazon ECS).	24 de outubro de 2024

Foi adicionado suporte para operações de GuardDuty CloudFormation tag	GuardDuty agora suporta a atualização da chave e do valor da tag e das tags no nível da pilha. Para fazer isso, adicione permissão `guardduty:tagResource` ao perfil do IAM. Para obter informações sobre GuardDuty CloudFormation, consulte a referência GuardDuty de tipo de recurso da Amazon no Guia AWS CloudFormation do usuário.	24 de outubro de 2024
Funcionalidade atualizada na Proteção contra GuardDuty Malware para S3	Ao ativar a proteção contra malware para S3, você pode escolher um perfil de serviço que tenha as permissões necessárias para realizar ações de verificação de malware em seu nome. Para obter mais informações sobre como habilitar a proteção contra malware para S3, consulte Configurando a proteção contra malware para S3 em seu bucket do S3.	22 de outubro de 2024

Funcionalidade atualizada	GuardDuty aprimora o tipo de UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.InsideAWSdescoberta para detectar o uso de credenciais de AWS instância do Amazon EC2 a partir de AWS PrivateLink endpoints de VPC (Contas da AWS) que não estão associados à função de instância do Amazon EC2. Esse novo GuardDuty recurso detecta o possível uso indevido das credenciais da instância Amazon EC2 e fornece o contexto do Conta da AWS controle remoto usando as credenciais da sessão de exfiltração. Para obter mais informações sobre endpoints de AWS serviço compatíveis com essa nova detecção, consulte Registro de eventos de atividade de rede no Guia do AWS CloudTrail usuário.	21 de outubro de 2024

Funcionalidade atualizada - Monitoramento GuardDuty de tempo de execução	GuardDuty O Runtime Monitoring adicionou os três tipos de descoberta a seguir que notificam você quando comandos suspeitos são executados em uma instância do Amazon EC2 ou carga de trabalho de contêiner em seu ambiente: AWS • Discovery:Runtime/SuspiciousCommand • Persistence:Runtime/SuspiciousCommand • PrivilegeEscalation:Runtime/SuspiciousCommand	10 de outubro de 2024
Novo recurso - Suporte adicionado aos endpoints da VPC	GuardDuty agora está integrado AWS PrivateLink e oferece suporte a endpoints VPC. Para obter mais informações sobre a AWS PrivateLink integração, consulte Amazon GuardDuty e a interface VPC endpoints ().AWS PrivateLink	17 de setembro de 2024
Funcionalidade atualizada no Runtime Monitoring - Amazon EKS	O Runtime Monitoring lançou uma nova versão de atendente 1.7.1 para recursos do Amazon EKS. Para obter mais informações sobre as notas de lançamento, consulte o agente GuardDuty de segurança do Amazon EKS.	13 de setembro de 2024

Atualização da funcionalidade na Proteção contra Malware para S3	O Malware Protection for S3 adicionou um novo campo,`s3Throttled` , ao esquema Amazon EventBridge (EventBridge) de resultados da verificação de objetos do S3. O campo `s3Throttled` indica se houve ou não um atraso no upload ou na recuperação do armazenamento dos buckets do Amazon Simple Storage Service (Amazon S3). Para obter mais informações, consulte Monitoramento de escaneamentos de objetos do S3 com a Amazon. EventBridge	13 de setembro de 2024
Funcionalidade atualizada no Runtime Monitoring - Amazon EC2	O Runtime Monitoring lançou uma nova versão de atendente 1.3.1 para recursos do Amazon EC2. Para obter mais informações sobre as notas de lançamento, consulte o agente GuardDuty de segurança do Amazon EC2.	12 de setembro de 2024

Funcionalidade atualizada no monitoramento de tempo de execução - Amazon ECS-Fargate	O Runtime Monitoring lançou uma nova versão 1.3.1 do agente para ECS-Fargate recursos da Amazon. Para obter mais informações sobre as notas de lançamento, consulte o agente de GuardDuty segurança para AWS Fargate (somente Amazon ECS).	11 de setembro de 2024
Função GuardDuty vinculada ao serviço (SLR) atualizada	GuardDuty atualizou a SLR para incluir a `ec2:DescribeVpcs` permissão nas ações do Amazon EC2. Para obter mais informações, consulte permissões de Service-linked função para GuardDuty.	22 de agosto de 2024

Adição de conteúdo significativo	GuardDuty adicionou atualizações de conteúdo significativas ao recurso Malware Protection for S3. • Foram adicionados novos exemplos de esquema de notificação para configurar EventBridge as regras da Amazon para receber notificações relacionadas ao status do recurso do plano de Proteção contra Malware e ao resultado da verificação de objetos do S3. Para obter mais informações, consulte Monitoramento de escaneamentos de objetos do S3 com a Amazon. EventBridge • Foram adicionadas informações sobre a solução de problemas de falhas na tag pós-digitalização de objetos do S3.	20 de agosto de 2024
Funcionalidade atualizada no monitoramento GuardDuty de tempo de execução - Amazon EC2	O Runtime Monitoring lançou uma nova versão de atendente 1.3.0 para recursos do Amazon EC2. Para obter mais informações sobre as notas de lançamento, consulte o agente GuardDuty de segurança do Amazon EC2.	19 de agosto de 2024

Funcionalidade atualizada no monitoramento GuardDuty de tempo de execução - Amazon EKS	O Runtime Monitoring lançou uma nova versão de atendente 1.7.0 para recursos do Amazon EKS. Para obter mais informações sobre as notas de lançamento, consulte o agente GuardDuty de segurança para clusters do Amazon EKS.	17 de agosto de 2024
Adição de conteúdo significativo	GuardDuty adicionou novas informações sobre a metodologia de detecção de malware e os mecanismos de verificação que ela usa para os recursos Malware Protection for S3 e Malware Protection for EC2. Para obter mais informações, consulte Mecanismo de verificação de detecção de GuardDuty malware.	15 de agosto de 2024
Novo recurso - Protegendo cargas de trabalho de IA	GuardDuty A detecção básica de ameaças e a Proteção Lambda ajudam você a proteger e detectar melhor as ameaças às cargas de trabalho de IA incorpora das. AWS Para obter mais informações, consulte Protegendo cargas de trabalho de IA com GuardDuty.	14 de agosto de 2024

Funcionalidade atualizada no GuardDuty Runtime Monitoring - Fargate (somente Amazon ECS)	O Runtime Monitoring lançou uma nova versão 1.3.0 do agente para AWS Fargate recursos (somente Amazon ECS). Para obter mais informações sobre as notas de versão, consulte o agente GuardDuty de segurança para Fargate-ECS.	9 de agosto de 2024
Atualização da funcionalidade - Proteção contra Malware para S3	GuardDuty A proteção contra malware para S3 aumenta a cota do número máximo de buckets do S3 de 10 para 25 buckets. Essa cota se aplica a um Conta da AWS por cada Região da AWS. Para obter mais informações, consulte Proteção contra Malware para S3.	8 de agosto de 2024
Atualizado - Novos tipos de descoberta no Monitoramento de Runtime	GuardDuty adicionou dois novos tipos de descoberta do Runtime Monitoring que ajudarão você a detectar ameaças envolvendo a criação suspeita de shell no recurso monitorado e o escalonamento de privilégios em que um processo eleva suspeitamente seus privilégios à raiz. • Execution:Runtime/SuspiciousShellCreated • PrivilegeEscalation:Runtime/ElevationToRoot	6 de agosto de 2024

Atualizado - Integração com AWS Security Hub CSPM	AWS Security Hub CSPM fornece uma lista de controles de GuardDuty segurança para avaliar seus recursos e verificar sua conformid ade com os padrões e as melhores práticas do setor de segurança. Para obter mais informações, consulte Usando GuardDuty controles no CSPM do Security Hub.	11 de julho de 2024
Script GuardDuty de testador atualizado para descobertas	GuardDuty agora oferece suporte a mais de 100 descobertas com AWS recursos diferentes em uma conta dedicada. Para obter mais informações, consulte GuardDuty Resultados do teste em contas dedicadas.	28 de junho de 2024

Funcionalidade atualizada no Monitoramento de runtime	O Monitoramento de Runtime lançou uma nova versão de atendente 1.2.0 para recursos do Amazon EC2. Para obter informações sobre as notas de lançamento, consulte o agente GuardDuty de segurança para a instância do Amazon EC2. Para obter informações sobre como atualizar manualmente o atendente de segurança para esta versão de lançamento, consulte Gerenciando o atendente de segurança manualmente para a instância do Amazon EC2.	13 de junho de 2024
Novo recurso - Disponibilidade da proteção contra malware para a região S3	GuardDuty A proteção contra malware para S3 agora está disponível em todas as regiões comerciais em que GuardDuty está disponível. Esse recurso ajuda você a escanear objetos recém-carregados nos buckets do Amazon S3 em busca de possíveis malwares e uploads suspeitos e a tomar medidas para isolá-los antes que sejam ingeridos em processos posteriores. Para obter informações sobre como ativar a Proteção contra Malware para o S3, consulte Proteção contra GuardDuty malware para o S3.	12 de junho de 2024

Novo recurso - Proteção contra malware para S3	GuardDuty anuncia a disponibilidade geral do Malware Protection for S3, que ajuda você a escanear objetos recém-carregados nos buckets do Amazon S3 em busca de possíveis malwares e uploads suspeitos e a tomar medidas para isolá-los antes que sejam ingeridos em processos posteriores. Esse recurso é totalmente gerenciado pelo AWS. GuardDuty publica o resultado da verificação de objetos do S3 em seu barramento de eventos EventBridge padrão. Você pode permitir GuardDuty a adição de tags aos objetos digitalizados do S3. Você pode criar fluxos de trabalho downstream, como isolamento de um bucket de quarentena, ou definir políticas de bucket usando tags que impedem que usuários ou aplicativos acessem determinados objetos. Para obter mais informações, consulte GuardDuty Proteção contra Malware para S3. Atualmente, ele está disponível nas seguintes regiões: • Leste dos EUA (Norte da Virgínia)	11 de junho de 2024

	• Leste dos EUA (Ohio) • Oeste dos EUA (Oregon) • Europa (Irlanda) • Europa (Frankfurt) • Europa (Estocolmo) • Ásia-Pacífico (Sydney) • Ásia-Pacífico (Tóquio) • Ásia-Pacífico (Singapura)	
Política AmazonGuardDutyFullAccess atualizada	Permissão adicionada que permite passar uma função do IAM para GuardDuty quando você ativa a Proteção contra Malware para S3. Para obter mais informações sobre essa atualização de política, consulte a política gerenciada pela AWS : AmazonGuardDutyFullAccess.	10 de junho de 2024
Funcionalidade atualizada no GuardDuty RDS Protection	A Proteção RDS amplia o suporte para monitorar a atividade de login em seus bancos de dados RDS para PostgreSQL. Como parte dessa expansão, GuardDuty começará automaticamente a monitorar os dados de login do RDS para bancos de dados PostgreSQL para contas que já habilitaram a Proteção do RDS. GuardDuty Para obter mais informações, consulte Proteção RDS.	6 de junho de 2024

Funcionalidade atualizada no GuardDuty Runtime Monitoring - Fargate (somente Amazon ECS)	O Runtime Monitoring lançou uma nova versão 1.2.0 do agente para AWS Fargate recursos (somente Amazon ECS). Para obter mais informações sobre as notas de versão, consulte o agente GuardDuty de segurança para Fargate-ECS.	31 de maio de 2024
Funcionalidade atualizada na proteção contra GuardDuty malware para EC2	Para cada volume do Amazon EBS anexado às suas instâncias e cargas de trabalho de contêineres do Amazon EC2 GuardDuty , o Malware Protection for EC2 aumentou o tamanho do volume do EBS que ele verifica para até 2048 GB. Para obter informações sobre como escanear volumes do Amazon EBS anexados às suas instâncias, consulte Proteção contra GuardDuty malware para EC2.	29 de maio de 2024

Funcionalidade atualizada no Monitoramento de runtime	O Runtime Monitoring for Amazon ECS-Fargate agora oferece suporte à detecção de possíveis ameaças em suas tarefas iniciadas por AWS Batch e. AWS CodePipeline Para obter mais informações, consulte Como o Monitoramento Runtime funciona com Fargate (Amazon EC2 somente).	28 de maio de 2024
Funcionalidade atualizada no Monitoramento de runtime	O Monitoramento de Runtime lançou uma nova versão de atendente 1.6.1 para recursos do Amazon EKS. Para obter mais informações, consulte o Histórico de versões do atendente complementar do EKS.	14 de maio de 2024
Suporte regional expandido para Runtime Monitoring	GuardDuty expande o suporte ao monitoramento de tempo de execução para a região Oeste do Canadá (Calgary) . Para obter informações sobre como começar a usar o Runtime Monitoring, consulte Habilitando o Runtime Monitoring.	7 de maio de 2024

Suporte regional expandido para proteção do RDS	GuardDuty expande o suporte ao RDS Protection para o seguinte: Regiões da AWS • Oeste do Canadá (Calgary) • Ásia-Pacífico (Hyderabad) • Europa (Espanha) • Europa (Zurique) • Oriente Médio (Emirados Árabes Unidos) • Israel (Tel Aviv) • Ásia-Pacífico (Melbourne) Para obter informações sobre como ativar esse recurso, consulte Proteção do RDS.	3 de maio de 2024
Funcionalidade atualizada no Monitoramento de runtime	O Runtime Monitoring lançou uma nova versão 1.1.0 do agente para AWS Fargate recursos (somente Amazon ECS). Para obter mais informações sobre as notas de versão, consulte o agente GuardDuty de segurança para Fargate-ECS.	1º. de maio de 2024
Funcionalidade atualizada no Monitoramento de runtime	O Monitoramento de Runtime lançou uma nova versão de atendente 1.6.0 para recursos do Amazon EKS. Para obter mais informações, consulte o Histórico de versões do atendente complementar do EKS.	29 de abril de 2024

Suporte para IPAddressV6	GuardDuty adicionou suporte ao IPAddressV6 para detalhes de IP local e remoto. Você pode usar os atributos de filtro associados para filtrar GuardDuty descobertas ou criar regras de supressão.	18 de abril de 2024
Experiência de console atualizada para configurar as descobertas de exportação	GuardDuty atualizou a experiência do console para exportar as descobertas geradas em seu Contas da AWS, para um bucket do Amazon S3. Para obter mais informações, consulte Exportação de GuardDuty descobertas.	1º de abril de 2024
Funcionalidade atualizada no Monitoramento de runtime	O Monitoramento de Runtime lançou uma nova versão de atendente 1.1.0 para recursos do Amazon EC2. Esta versão oferece suporte à configura ção GuardDuty automatiz ada de agentes no Runtime Monitoring para instâncias do Amazon EC2. Para obter informações sobre as notas de lançamento, consulte o agente GuardDuty de segurança para a instância do Amazon EC2.	28 de março de 2024

Disponibilidade geral do Runtime Monitoring para instâncias do Amazon EC2	GuardDuty anuncia a disponibilidade geral (GA) do Runtime Monitoring para instâncias do Amazon EC2. Agora, você tem a opção de ativar a configuração automática do agente que permite GuardDuty instalar e gerenciar o agente de segurança para suas instâncias do Amazon EC2 em seu nome. Com o agente GuardDuty automatizado, você também pode usar tags de inclusão ou exclusão GuardDuty para informar a instalação e o gerenciamento do agente de segurança somente em instâncias selecionadas do Amazon EC2. Para obter mais informações, consulte How Runtime Monitoring works with Amazon EC2 instances. Lista de novos tipos de descobertas lançados junto com este GA • Execution:Runtime/SuspiciousTool • Execution:Runtime/SuspiciousCommand • DefenseEvasion:Runtime/SuspiciousCommand • DefenseEvasion:Runtime/PtraceAntiDebugging	28 de março de 2024

- Execution:Runtime/MaliciousFileExecuted

A Amazon GuardDuty atualizou a Service-linked função (SLR)	Use AWS Systems Manager ações para gerenciar associações de SSM em instâncias do Amazon EC2 ao GuardDuty habilitar o Runtime Monitoring com agente automatizado para o Amazon EC2. Quando a configuração GuardDuty automatizada do agente está desativada, GuardDuty considera somente as instâncias do EC2 que têm uma tag de inclusão (`GuardDuty Managed :true`). • A lista a seguir mostra as novas permissões: `"ssm:DescribeAssociation", "ssm:DeleteAssociation", "ssm:UpdateAssociation", "ssm:CreateAssociation", "ssm:StartAssociationsOnce", "ssm:AddTagsToResource", "ssm:CreateAssociation", "ssm:UpdateAssociation", "ssm:SendCommand", "ssm:GetCommandInvocation"`	26 de março de 2024

Funcionalidade atualizada no Monitoramento de runtime	Com a versão mais recente do agente de GuardDuty segurança (complemento) v1.5.0 para o Amazon EKS, o Runtime Monitoring agora oferece suporte à configura ção de parâmetros específicos do seu agente de GuardDuty segurança, como configura ções de CPU e memória, `PriorityClass` configura ções e configurações de política de DNS. Para obter mais informações, consulte Configuração dos parâmetro s do agente GuardDuty de segurança (complemento EKS).	7 de março de 2024
Funcionalidade atualizada no Monitoramento de runtime	O Monitoramento de Runtime lançou uma nova versão de atendente 1.5.0 para recursos do Amazon EKS. Para obter mais informações, consulte o Histórico de versões do atendente complementar do EKS.	7 de março de 2024

Suporte para a região Oeste do Canadá (Calgary)	A Amazon agora GuardDuty está disponível na região Oeste do Canadá (Calgary). Alguns dos planos de proteção incluídos GuardDuty podem não estar disponíveis nesta região. Para obter mais informações, consulte Regiões e endpoints.	6 de março de 2024
Funcionalidade atualizada no Monitoramento de runtime	As versões 1.0.0 e 1.1.0 do agente de GuardDuty segurança para clusters Amazon EKS não serão mais suportadas a partir de 14 de maio de 2024. Para obter informações sobre quais etapas você pode tomar antes do final do suporte padrão, consulte o agente GuardDuty de segurança para clusters do Amazon EKS.	16 de fevereiro de 2024

Funcionalidade atualizada no Monitoramento de runtime	O Monitoramento de Runtime é compatível com a versão 1.29 mais recente do Kubernetes com a versão 1.4.1 do atendente de segurança existente. O suporte está disponível desde o lançamento desta versão do Kubernetes. Para obter informações sobre as versões compatíveis do Kubernetes, consulte Versões do Kubernetes suportadas pelo agente de segurança. GuardDuty	16 de fevereiro de 2024

Funcionalidade atualizada no Monitoramento de Runtime - Disponibilidade regional	GuardDuty O Runtime Monitoring agora oferece suporte ao Amazon VPC compartilhado dentro do mesmo. AWS Organizations GuardDuty a função vinculada ao serviço (SLR) tem uma nova permissão, `organizations:DescribeOrganization` que ajuda a recuperar o ID da organização da conta compartilhada da Amazon VPC para definir a política de endpoint. Para obter informações sobre os pré-requisitos para usar um endpoint compartilhado da Amazon VPC no Monitoramento de Runtime, consulte Support for shared Amazon VPC. Esse recurso está disponível em todas as regiões que oferecem GuardDuty suporte ao monitoramento de tempo de execução.	12 de fevereiro de 2024

Funcionalidade atualizada no Monitoramento de Runtime - Disponibilidade regional	GuardDuty O Runtime Monitoring agora oferece suporte ao Amazon VPC compartilhado dentro do mesmo. AWS Organizations GuardDuty a função vinculada ao serviço (SLR) tem uma nova permissão, `organizations:DescribeOrganization` que ajuda a recuperar o ID da organização da conta compartilhada da Amazon VPC para definir a política de endpoint. Para obter informações sobre os pré-requisitos para usar um endpoint compartilhado da Amazon VPC no Monitoramento de Runtime, consulte Support for shared Amazon VPC. Atualmente, esse recurso está disponível em alguns dos Regiões da AWS. Para obter mais informações, consulte Regiões e endpoints da .	9 de fevereiro de 2024
Funcionalidade atualizada com suporte para o novo Regiões da AWS — Proteção contra malware para EC2	O Malware Protection for EC2 agora suporta a verificação dos volumes do EBS criptografados Chaves gerenciadas pela AWS na região Oeste dos EUA (Oregon).	6 de fevereiro de 2024

Funcionalidade atualizada com suporte para o novo Regiões da AWS — Proteção contra malware para EC2	O Malware Protection for EC2 agora suporta a verificação dos volumes do EBS Chaves gerenciadas pela AWS criptografados com o seguinte: Regiões da AWS • Ásia-Pacífico (Singapura) (`ap-southeast-1`) • Europa (Frankfurt) (`eu-central-1`) • Asia-Pacífico (Osaka) (`ap-northeast-3`) • Leste dos EUA (Ohio) (`us-east-2`) • Europa (Milão) (`eu-south-1`) • Ásia-Pacífico (Tóquio) (`ap-northeast-1`) • Ásia-Pacífico (Seul) (`ap-northeast-2`) • Canadá (Central) (`ca-central-1`) • Europa (Irlanda) (`eu-west-1`) • Leste dos EUA (Norte da Virgínia) (`us-east-1`)	5 de fevereiro de 2024

Funcionalidade atualizada no Monitoramento de runtime	GuardDuty O Runtime Monitoring lançou uma nova versão do agente de GuardDuty segurança (v1.0.2) para instâncias do Amazon EC2. Essa versão do atendente inclui suporte para as AMIs mais recentes do Amazon ECS. Para obter mais informações sobre o histórico de lançamentos de agentes, consulte Agente GuardDuty de segurança para instâncias do Amazon EC2.	2 de fevereiro de 2024

Funcionalidade atualizada com suporte para o novo Regiões da AWS — Proteção contra malware para EC2	O Malware Protection for EC2 agora suporta a verificação dos volumes do Amazon EBS Chaves gerenciadas pela AWS criptografados com o seguinte: Regiões da AWS • Europa (Londres) (`eu-west-2`) • Europa (Estocolmo) (`eu-north-1`) • Ásia-Pacífico (Hong Kong) (`ap-east-1`) • África (Cidade do Cabo) (`af-south-1`) • Oriente Médio (Bahrein) (`me-south-1`) • Ásia-Pacífico (Hyderabad) (`ap-south-2`) • Europa (Espanha) (`eu-south-2`) • Ásia-Pacífico (Melbourne) (`ap-southeast-4`) • Ásia-Pacífico (Sydney) (`ap-southeast-2`) • Israel (Tel Aviv) (`il-central-1`)	31 de janeiro de 2024

Gerenciamento de contas atualizado com AWS Organizations	Reorganizou o conteúdo em Gerenciando contas com AWS Organizations. , adicionou etapas para alterar a conta do GuardDuty administrador delegado e atualizou Compreendendo a relação entre a conta do GuardDuty administrador e as contas dos membros.	30 de janeiro de 2024
Funcionalidade atualizada com suporte para novos Regiões da AWS	O Malware Protection for EC2 agora suporta a verificação dos volumes do EBS Chaves gerenciadas pela AWS criptografados com o seguinte: Regiões da AWS • Ásia-Pacífico (Jacarta) (`ap-southeast-3`) • Oeste dos EUA (N. da Califórnia) (`us-west-1`) • Oriente Médio (Emirados Árabes Unidos) (`me-central-1`) • Europa (Zurique) (`eu-central-2`) • Ásia-Pacífico (Mumbai) (`ap-south-1`) • América do Sul (São Paulo) (`sa-east-1`)	29 de janeiro de 2024

Atualização da funcionalidade na Proteção contra Malware para EC2	A Proteção contra malware para EC2 agora suporta a verificação dos volumes do EBS criptografados com Chaves gerenciadas pela AWS. A proteção contra malware para o perfil vinculado ao serviço (SLR) do EC2 tem duas novas permissões — `GetSnapshotBlock` e `ListSnapshotBlocks`. Essas permissões ajudarão a GuardDuty obter o instantâneo de um volume do EBS (usando criptografia Chave gerenciada pela AWS) do seu Conta da AWS e copiá-lo para a conta de GuardDuty serviço antes de iniciar a verificação de malware. Atualmente, essa funcionalidade está disponível somente na região Europa (Paris) (`eu-west-3`). Para obter mais informações, consulte Volumes suportados para verificação de malware.	25 de janeiro de 2024

Funcionalidade atualizada no Monitoramento de runtime	GuardDuty O Runtime Monitoring lançou uma nova versão do agente de GuardDuty segurança (v1.0.1) com ajustes e aprimoramentos gerais de desempenho. Para obter mais informações sobre o histórico de lançamentos de agentes, consulte Agente GuardDuty de segurança para instâncias do Amazon EC2.	23 de janeiro de 2024
Funcionalidade atualizada no Monitoramento de runtime	O Monitoramento de Runtime lançou uma nova versão de atendente 1.4.1 para recursos do Amazon EKS. Para obter mais informações, consulte o Histórico de versões do agente complementar do EKS.	16 de janeiro de 2024
O Monitoramento de Runtime lançou uma nova versão de atendente 1.4.0 para recursos do Amazon EKS	O Monitoramento de Runtime lançou uma nova versão de atendente 1.4.0 para recursos do Amazon EKS. Para obter mais informações, consulte o Histórico de versões do agente complementar do EKS.	21 de dezembro de 2023

Foram adicionados tipos de descobertas baseadas em S3 e aprendizado de AWS CloudTrail máquina (ML) à Europa (Zurique), Europa (Espanha), Ásia-Pacífico (Hyderabad), Ásia-Pacífico (Melbourne) e Israel (Tel Aviv)	O seguinte S3 e as CloudTrail descobertas que identificam o comportamento anômalo usando o modelo de aprendizado GuardDuty de máquina (ML) de detecção de anomalias estão agora disponíveis nas regiões da Europa (Zurique), Europa (Espanha), Ásia-Pacífico (Hyderabad), Ásia-Pacífico (Melbourne) e Israel (Tel Aviv): • Discovery:S3/AnomalousBehavior • Impact:S3/AnomalousBehavior.Write • Impact:S3/AnomalousBehavior.Delete • Impact:S3/AnomalousBehavior.Permission • Exfiltration:S3/AnomalousBehavior • Exfiltration:IAMUser/AnomalousBehavior • Impact:IAMUser/AnomalousBehavior • CredentialAccess:IAMUser/AnomalousBehavior • DefenseEvasion:IAMUser/AnomalousBehavior • InitialAccess:IAMUser/AnomalousBehavior	21 de dezembro de 2023

	• Persistence:IAMUser/AnomalousBehavior • PrivilegeEscalation:IAMUser/AnomalousBehavior • Discovery:IAMUser/AnomalousBehavior	
GuardDuty suporta 50.000 contas de membros por meio de AWS Organizations	Agora, um GuardDuty administrador delegado pode gerenciar no máximo 50.000 contas de membros por meio do. AWS Organizations Isso também inclui um máximo de 5000 contas de membros associadas à conta de GuardDuty administrador por convite.	20 de dezembro de 2023

GuardDuty Suporte de monitoramento de tempo de execução expandido para 19 Regiões da AWS	O Monitoramento de runtime está disponível na Ásia-Pacífico (Jacarta), Europa (Paris), Ásia-Pacífico (Osaka), Ásia-Pacífico (Seul), Oriente Médio (Bahrein), Ásia-Pacífico (Hyderabad), Ásia-Pacífico (Melbourne), Israel (Tel Aviv), Oeste dos EUA (Norte da Califórnia), Ásia-Pacífico (Hong Kong), Europa (Tel Aviv), Oeste dos EUA (Norte da Califórnia), Ásia-Pacífico (Hong Kong), Europa (Tel Aviv), Oeste dos EUA (Norte da Califórnia), Ásia-Pacífico (Hong Kong), Europa (Tel Aviv), Oeste dos EUA (Norte da Califórnia), Ásia-Pacífico (Hong Kong), Europa (Tel Aviv), Oeste dos EUA (Norte da Califórnia), América do Sul (São Paulo), Ásia-Pacífico (Mumbai), Canadá (Central), África (Cidade do Cabo), Europa (Zurique).	6 de dezembro de 2023

GuardDuty expande a capacidade de monitoramento de tempo de execução	Além de detectar ameaças aos seus clusters do Amazon EKS, GuardDuty anuncia a disponibilidade geral do Runtime Monitoring para detectar ameaças às suas cargas de trabalho do Amazon ECS e uma versão prévia para detectar ameaças às suas instâncias do Amazon EC2. Para obter mais informações sobre quais Regiões da AWS atualmente oferecem suporte ao Monitoramento de Runtime, consulte Regiões e endpoints.	26 de novembro de 2023

A Amazon GuardDuty atualizou a Service-linked função (SLR)	GuardDuty adicionou novas permissões para usar as ações do Amazon ECS para gerenciar e recuperar informações sobre os clusters do Amazon ECS e gerenciar a configuração da conta do Amazon ECS com. `guarddutyActivate` As ações relacionadas ao Amazon ECS também recuperam as informações sobre as tags associadas a. GuardDuty • As seguintes permissões foram adicionadas como parte da GuardDuty expansão do recurso de monitoramento de tempo de execução: `"ecs:ListClusters", "ecs:DescribeClusters", "ecs:PutAccountSettingDefault"`	26 de novembro de 2023
Atualizou as políticas AWS gerenciadas	GuardDuty adicionou uma nova permissão `organizations:ListAccounts` à política AWS gerenciada: AmazonGuardDutyFullAccessAmazonGuardDutyReadOnlyAccesse.	16 de novembro de 2023

GuardDuty lançou novos tipos de descoberta que usam o EKS Audit Log Monitoring.	O Monitoramento de logs de auditoria do EKS agora é compatível com os seguintes tipos de descoberta na Ásia-Pacífico (Melbourne) (`ap-southeast-4`). • CredentialAccess:Kubernetes/AnomalousBehavior.SecretsAccessed • PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleBindingCreated • Execution:Kubernetes/AnomalousBehavior.ExecInPod • PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!PrivilegedContainer • PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!ContainerWithSensitiveMount • Execution:Kubernetes/AnomalousBehavior.WorkloadDeployed • PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleCreated • Discovery:Kubernetes/AnomalousBehavior.PermissionChecked	11 de novembro de 2023

GuardDuty lançou novos tipos de descoberta que usam o EKS Audit Log Monitoring.	O Monitoramento de logs de auditoria do EKS agora suporta os seguintes tipos de descoberta nas regiões Ásia-Pacífico (Hyderabad (`ap-south-2`), Europa (Zurique) (`eu-central-2`) e Europa (Espanha) (`eu-south-2`). • CredentialAccess:Kubernetes/AnomalousBehavior.SecretsAccessed • PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleBindingCreated • Execution:Kubernetes/AnomalousBehavior.ExecInPod • PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!PrivilegedContainer • PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!ContainerWithSensitiveMount • Execution:Kubernetes/AnomalousBehavior.WorkloadDeployed • PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleCreated	10 de novembro de 2023

- Discovery:Kubernetes/AnomalousBehavior.PermissionChecked

GuardDuty lançou novos tipos de descoberta que usam o EKS Audit Log Monitoring.	O Monitoramento de logs de auditoria do EKS agora é compatível com os seguintes tipos de descoberta. Os seguintes tipos de descobert a ainda não estão disponíve is nas Regiões Ásia-Pacífico (Hyderabad) (`ap-south-2`), Europa (Zurique) (`eu-centra l-2`), Europa (Espanha) (`eu-south-2`) e Ásia-Pací fico (Melbourne) (`ap-southe ast-4`): • CredentialAccess:K ubernetes/Anomalou sBehavior.SecretsAccessed • PrivilegeEscalation:Kuberne tes/AnomalousBehav ior.RoleBindingCreated • Execution:Kubernetes/ AnomalousBehavior.ExecIn Pod • PrivilegeEscalation:Kuberne tes/AnomalousBehav ior.WorkloadDeployed!Privil egedContainer • PrivilegeEscalation:Kuberne tes/AnomalousBehav ior.WorkloadDeployed! ContainerWithSensitiveMo unt • Execution:Kubernetes/ AnomalousBehavior.Worklo adDeployed	8 de novembro de 2023

	• PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleCreated • Discovery:Kubernetes/AnomalousBehavior.PermissionChecked	
O Monitoramento de runtime do EKS lançou o novo atendente v1.3.1	O Monitoramento de runtime do EKS lançou uma nova versão 1.3.1 do atendente que inclui patches e atualizações de segurança importantes.	23 de outubro de 2023
Novo atributo de filtro para descoberta	GuardDuty adicionou um novo critério para filtrar as descobertas geradas. O sufixo do domínio de solicitação de DNS fornece o domínio de segundo e primeiro nível envolvido na atividade que solicitou GuardDuty a geração da descoberta.	17 de outubro de 2023
O Monitoramento de runtime do EKS lançou o novo atendente v1.3.0 compatível com a versão 1.28 do Kubernetes	O Monitoramento de runtime do EKS lançou uma nova versão 1.3.0 do atendente que oferece suporte à versão 1.28 do Kubernetes. Foi adicionado o suporte para Ubuntu. Para obter mais informações, consulte o Histórico de versões do agente complementar do EKS.	5 de outubro de 2023

Foram adicionados tipos de descobertas baseadas em S3 e aprendizado de AWS CloudTrail máquina (ML) às regiões Ásia-Pacífico (Jacarta) e Oriente Médio (EAU)	O seguinte S3 e as CloudTrail descobertas que identificam o comportamento anômalo usando o modelo de aprendizado GuardDuty de máquina (ML) de detecção de anomalias estão agora disponíveis nas regiões Ásia-Pacífico (Jacarta) e Oriente Médio (EAU): • Discovery:S3/AnomalousBehavior • Impact:S3/AnomalousBehavior.Write • Impact:S3/AnomalousBehavior.Delete • Impact:S3/AnomalousBehavior.Permission • Exfiltration:S3/AnomalousBehavior • Exfiltration:IAMUser/AnomalousBehavior • Impact:IAMUser/AnomalousBehavior • CredentialAccess:IAMUser/AnomalousBehavior • DefenseEvasion:IAMUser/AnomalousBehavior • InitialAccess:IAMUser/AnomalousBehavior • Persistence:IAMUser/AnomalousBehavior	20 de setembro de 2023

	• PrivilegeEscalation:IAMUser/AnomalousBehavior • Discovery:IAMUser/AnomalousBehavior	
GuardDuty O EKS Runtime Monitoring apresenta o gerenciamento GuardDuty de agentes de segurança no nível do cluster	O EKS Runtime Monitoring adiciona suporte para gerenciar o agente de GuardDuty segurança para clusters EKS individuais para monitorar os eventos de tempo de execução somente desses clusters seletivos. O Monitoramento de runtime do EKS amplia esse recurso com o suporte de tags.	13 de setembro de 2023
GuardDuty A proteção contra malware para EC2 estende o suporte a mais Regiões da AWS	A Proteção contra malware para EC2 está disponível na Ásia-Pacífico (Hyderabad), Ásia-Pacífico (Melbourne), Europa (Zurique) e Europa (Espanha).	11 de setembro de 2023

GuardDuty agora está disponível na região de Israel (Tel Aviv)	Foi adicionada a região de Israel (Tel Aviv) à lista de Regiões da AWS onde agora GuardDuty está disponível. Os seguintes planos de proteção também estão disponíveis na região Israel (Tel Aviv): • O Proteção do EKS inclui Monitoramento de logs de auditoria do EKS e Monitoramento de runtime do EKS. • Proteção do Lambda. • Proteção contra malware para o EC2. • Proteção do S3. Para obter mais informaçõ es sobre a disponibilidade do plano de proteção na região Israel (Tel Aviv), consulte Regiões e endpoints.	24 de agosto de 2023
GuardDuty adicionou configuração de ativação automática para sua organizaç ão no nível do plano de proteção	Atualize a configuração da organização para os planos de proteção em sua região. As opções de configuração possíveis são habilitar para todas as contas, habilitar automaticamente para novas contas ou não habilitar automaticamente para nenhuma conta em sua organização.	16 de agosto de 2023

Os tipos de descoberta do S3 que identificam comportamentos anômalos usando o modelo de aprendizado GuardDuty de máquina (ML) de detecção de anomalias agora estão disponíveis na Ásia-Pacífico (Osaka)	Os seguintes tipos de descoberta estão disponíveis na região Ásia-Pacífico (Osaka): • Discovery:S3/AnomalousBehavior • Impact:S3/AnomalousBehavior.Write • Impact:S3/AnomalousBehavior.Delete • Impact:S3/AnomalousBehavior.Permission • Exfiltration:S3/AnomalousBehavior	10 de agosto de 2023
O Monitoramento de runtime do EKS está disponível na Ásia-Pacífico (Melbourne)	O EKS Runtime Monitoring dentro do GuardDuty EKS Protection fornece detecção de ameaças em tempo de execução para seus clusters Amazon EKS no AWS ambiente. Agora é compatível com a região Ásia-Pacífico (Melbourne).	8 de agosto de 2023
Atualizou a lista de GuardDuty descobertas que invocam a verificação de GuardDuty-initiated malware	Certos tipos de descoberta do EKS Runtime Monitoring agora podem invocar a verificação de GuardDuty -initiated malware em seu Conta da AWS.	19 de julho de 2023

GuardDuty suporta 10.000 contas de membros por meio de AWS Organizations	Agora, uma conta de GuardDuty administrador pode gerenciar no máximo 10.000 contas de membros por meio de AWS Organizations. Isso também inclui um máximo de 5000 contas de membros associadas à conta de GuardDuty administrador por convite.	29 de junho de 2023
O Monitoramento de runtime do EKS anuncia três novos tipos de descoberta.	O Monitoramento de runtime do EKS oferece suporte a três novos tipos de descoberta baseados na técnica de injeção de processo. Os novos tipos de descoberta são DefenseEvasion:Runtime/ProcessInjection.Proc DefenseEvasion:Runtime/ProcessInjection.Ptrace, DefenseEvasion:Runtime/ProcessInjection.VirtualMemoryWrite e.	22 de junho de 2023
O Monitoramento de runtime do EKS lançou o novo atendente v1.2.0 que suporta a versão 1.27 do Kubernetes	O EKS Runtime Monitoring lançou uma nova versão 1.2.0 do agente que também oferece suporte a ARM64-based instâncias. Foi adicionado o suporte para Bottlerocket. Para obter mais informações, consulte o Histórico de versões do agente complementar do EKS.	16 de junho de 2023

GuardDuty O console fornece uma visão resumida de suas descobertas.	O painel de resumo no GuardDuty console fornece uma visão agregada das GuardDuty descobertas. Atualmente, o painel exibe dados por meio de vários widgets das últimas 10.000 descobertas geradas para sua conta (ou contas de membros, se você for uma conta de GuardDuty administrador) para a região atual.	12 de junho de 2023
O Monitoramento de logs de auditoria do EKS está disponível na Ásia-Pacífico (Hyderabad), Ásia-Pacífico (Melbourne), Ásia-Pacífico (Melbourne), Europa (Zurique) e Europa (Espanha)	Habilite o Monitoramento de logs de auditoria do EKS (na Proteção do EKS) para que suas contas monitorem os logs de auditoria do Kubernetes dos seus clusters do Amazon EKS e analise-os em busca de atividade s potencialmente mal-inten cionadas e suspeitas.	1º de junho de 2023
O Monitoramento de logs de auditoria do EKS está disponível no Oriente Médio (EAU)	O Monitoramento de logs de auditoria do EKS está disponível no Oriente Médio (EAU) Habilite o Monitoram ento de logs de auditoria do EKS para que suas contas monitorem os logs de auditoria do EKS dos seus clusters do Amazon EKS e analise-os em busca de atividades potencial mente mal-intencionadas e suspeitas.	3 de maio de 2023

GuardDuty O Malware Protection for EC2 anuncia On-demand a verificação de malware	A Proteção contra malware para EC2 ajuda a detectar a possível presença de malware nos volumes do Amazon EBS anexados às suas instâncias do Amazon EC2 e às workloads de contêiner es. Agora, ele oferece dois tipos de escaneamentos: GuardDuty iniciados e sob demanda. GuardDuty-initiated o escaneamento de malware inicia automaticamente um escaneamento sem agente nos volumes do Amazon EBS somente quando GuardDuty gera uma das descobertas que invocam o escaneame nto de malware. GuardDuty-initiated Você pode iniciar uma verificação de On-demand malware para instâncias do Amazon EC2 em sua conta fornecendo o Amazon Resource Name (ARN) associado a essa instância do Amazon EC2. Para obter mais informações sobre como os dois tipos de verificação diferem, consulte Proteção contra malware. • GuardDuty-initiated escaneamento de malware • On-demand escaneamento de malware	27 de abril de 2023

GuardDuty anuncia a Proteção Lambda	A Proteção do Lambda ajuda você a identificar possíveis ameaças à segurança em suas funções do AWS Lambda . • Tipos de descoberta da Proteção do Lambda • Correção de uma função do Lambda comprometida	20 de abril de 2023
GuardDuty agora está disponível na região Ásia-Pacífico (Melbourne)	Foi adicionada a região Ásia-Pacífico (Melbourne) à lista de Regiões da AWS onde GuardDuty está disponível. Para obter informações sobre quais recursos estão disponíveis na região, consulte Regiões e endpoints.	19 de abril de 2023
GuardDuty adicionou 3 novos tipos de descobertas do EC2	GuardDuty apresenta novos tipos de descoberta para detectar o uso de resolvedores de DNS externos e tecnologias de DNS criptografadas. Para obter informações sobre Regiões da AWS onde esses tipos de descoberta são compatíveis, consulte Regiões e endpoints. • DefenseEvasion:EC2/UnusualDNSResolver • DefenseEvasion:EC2/UnusualDoHActivity • DefenseEvasion:EC2/UnusualDoTActivity	5 de abril de 2023

GuardDuty anuncia o EKS Runtime Monitoring na EKS Protection	O EKS Runtime Monitoring dentro do EKS Protection fornece detecção de ameaças em tempo de execução para seus clusters Amazon EKS no AWS ambiente. Ele usa um atendente complementar do Amazon EKS (`aws-guardduty-agent`) que coleta eventos de runtime de suas workloads do EKS. Depois de GuardDuty receber esses eventos de tempo de execução, ele os monitora e analisa para identificar possíveis ameaças suspeitas à segurança. Para obter mais informações, consulte Como encontrar detalhes e Tipos de descoberta do Monitoramento de runtime do EKS.	30 de março de 2023

GuardDuty adiciona uma nova funcionalidade — `autoEnableOrganizationMembers`	GuardDuty A Amazon adiciona uma nova opção de configuração organizacional que ajuda as contas GuardDuty do administrador a auditar e aplicar (se necessário) o que GuardDuty está habilitado para `ALL` os membros de sua organização. A prática recomendada agora é usar `autoEnableOrganizationMembers` em vez de `autoEnable` . `autoEnable` está obsoleto, mas ainda é compatível. As seguintes APIs são afetadas por essa nova funcionalidade: • DescribeOrganizationConfiguration • UpdateOrganizationConfiguration • DisassociateMembers • DeleteMembers • DisassociateFromAdministratorAccount • StopMonitoringMembers	23 de março de 2023

O recurso RDS Protection na Amazon agora GuardDuty está disponível ao público em geral	GuardDuty O RDS Protection monitora e traça o perfil da atividade de login do RDS para identificar comportamentos suspeitos de login em suas instâncias de banco de dados Amazon Aurora. Para obter informações sobre quais Regiões da AWS oferecem suporte à Proteção do RDS, consulte Regiões e endpoints.	16 de março de 2023
GuardDuty anuncia a ativação do recurso	Historicamente, a GuardDuty API permitia a configuração de recursos e fontes de dados, mas agora, todos os novos tipos de GuardDuty proteção serão configurados como recursos e não como fontes de dados. GuardDuty ainda oferece suporte às fontes de dados via API, mas não adicionará uma nova API. A ativação de recursos afeta o comportamento das APIs usadas para habilitar GuardDuty ou um tipo de proteção dentro GuardDuty delas. Se você gerencia suas GuardDuty contas por meio de um modelo de API, SDK ou CFN, consulte as alterações GuardDuty da API em março de 2023.	16 de março de 2023

GuardDuty A proteção contra malware para EC2 agora está disponível na região do Oriente Médio (EAU)	O recurso Malware Protection for EC2 GuardDuty é suportado na região do Oriente Médio (EAU). Para obter mais informações, consulte Regiões e endpoints da .	13 de março de 2023
A Amazon GuardDuty atualizou a Service-linked função (SLR)	GuardDuty adicionou as seguintes novas permissões para oferecer suporte ao próximo recurso de monitoramento de tempo de execução do GuardDuty EKS. • Use as ações do Amazon EKS para gerenciar e recuperar informações sobre os clusters do EKS e gerenciar os complementos do EKS nos clusters do EKS. As ações do EKS também recuperam as informações sobre as tags associadas a. GuardDuty `"eks:ListClusters", "eks:DescribeCluster", "ec2:DescribeVpcEndpointServices", "ec2:DescribeSecurityGroups"`	8 de março de 2023

A Amazon GuardDuty atualizou a Service-linked função (SLR)	A GuardDuty SLR foi atualizada para permitir a criação da Proteção contra Malware para EC2 SLR após a ativação da Proteção contra Malware para EC2.	21 de fevereiro de 2023
GuardDuty requer TLS v1.2 ou posterior	Para se comunicar com AWS os recursos, GuardDuty requer e oferece suporte ao TLS v1.2 ou posterior. Para obter mais informações, consulte Proteção de dados e Segurança da infraestrutura.	14 de fevereiro de 2023
GuardDuty agora está disponível na região Ásia-Pacífico (Hyderabad)	Foi adicionada a região Ásia-Pacífico (Hyderabad) à lista de Regiões da AWS onde GuardDuty está disponível. Para obter mais informações, consulte Regiões e endpoints da .	14 de fevereiro de 2023
O Amazon GuardDuty User Guide está alinhado com as melhores práticas do IAM	Guia atualizado para alinhamento com as práticas recomendadas do IAM. Para saber mais, consulte Práticas recomendadas de segurança no IAM.	10 de fevereiro de 2023
GuardDuty agora está disponível na região Europa (Espanha)	A Europa (Espanha) foi adicionada à lista Regiões da AWS de GuardDuty onde está disponível. Para obter mais informações, consulte Regiões e endpoints da .	8 de fevereiro de 2023

GuardDuty agora está disponível na região Europa (Zurique)	A Europa (Zurique) foi adicionada à lista de Regiões da AWS onde GuardDuty está disponível. Para obter mais informações, consulte Regiões e endpoints da .	12 de dezembro de 2022
Versão prévia de um novo recurso — Proteção GuardDuty RDS	GuardDuty O RDS Protectio n monitora e traça o perfil da atividade de login do RDS para identificar comportam entos suspeitos de login em suas instâncias de banco de dados Amazon Aurora. Atualmente, ela está disponíve l para uma versão prévia em cinco Regiões da AWS. Para obter mais informações, consulte Regiões e endpoints da .	30 de novembro de 2022
GuardDuty agora está disponível na região do Oriente Médio (EAU)	O Oriente Médio (EAU) foi adicionado à lista de Regiões da AWS onde GuardDuty está disponível. Para obter mais informações, consulte Regiões e endpoints da .	6 de outubro de 2022

Conteúdo adicionado para um novo recurso — Proteção contra GuardDuty malware para EC2	GuardDuty A proteção contra malware para EC2 é um aprimoramento opcional da Amazon. GuardDuty Enquanto GuardDuty identifica os recursos em risco, o Malware Protection for EC2 detecta o malware que pode ser a fonte do comprometimento. Com o Malware Protectio n for EC2 ativado, sempre que GuardDuty detecta um comportamento suspeito em uma instância do Amazon EC2 ou em uma carga de trabalho de contêiner indicativ a de malware GuardDuty , o Malware Protection for EC2 inicia uma verificação sem agente nos volumes do EBS anexados às cargas de trabalho da instância ou contêiner do EC2 impactada s para detectar a presença de malware. Para obter informaçõ es sobre como a Proteção contra Malware para EC2 funciona e como configura r esse recurso, consulte Proteção contra GuardDuty malware para EC2. • Para obter informações sobre as descobertas da Proteção contra malware	26 de julho de 2022

	para EC2 , consulte Como encontrar detalhes. • Para obter informações sobre como remediar a instância EC2 comprometida e um contêiner autônomo, consulte Correção de problemas de segurança descobertos por. GuardDuty • Para obter informações sobre CloudWatch registros de auditoria para escaneamentos de malware e motivos para ignorar um recurso durante o escaneamento de malware, consulte Entendendo CloudWatch registros e motivos para ignorar os motivos. • Para obter informações sobre detecções de ameaças de falsos positivos , consulte Relatar falsos positivos no GuardDuty Malware Protection for EC2.	
Um tipo de descoberta foi retirado	Exfiltration:S3/ObjectRead.Unusual foi retirado.	5 de julho de 2022

Foram adicionados novos tipos de descoberta do S3 que identificam comportamentos anômalos usando o modelo de aprendizado GuardDuty de máquina (ML) de detecção de anomalias.	Foram adicionados os novos tipos de descoberta do S3 a seguir. Esses tipos de descoberta identificam se uma solicitação de API invocou uma entidade do IAM de forma anômala. O modelo de ML avalia todas as solicitações de API em sua conta e identifica eventos anômalos associados às técnicas usadas pelos adversários. Para saber mais sobre cada uma dessas novas descobertas, consulte Tipos de descoberta do S3. • Discovery:S3/AnomalousBehavior • Impact:S3/AnomalousBehavior.Write • Impact:S3/AnomalousBehavior.Delete • Impact:S3/AnomalousBehavior.Permission • Exfiltration:S3/AnomalousBehavior	5 de julho de 2022

Conteúdo de proteção GuardDuty EKS adicionado para GuardDuty	GuardDuty agora pode gerar descobertas para seus recursos do Amazon EKS por meio do monitoramento dos registros de auditoria do EKS. Para saber como configura r esse recurso, consulte Proteção EKS na Amazon GuardDuty. Para obter uma lista das descobertas que GuardDuty podem ser geradas para os recursos do Amazon EKS, consulte as descobert as do Kubernetes. Uma nova orientação de remediação foi adicionada para apoiar a remediação dessas descobert as no guia de descoberta de remediação do Kubernetes.	25 de janeiro de 2022
Foi adicionada 1 nova descoberta	Uma nova descoberta, UnauthorizedAccess:IAMUser/ InstanceCredentialExfiltrat ion.InsideAWS, foi adicionad a. Essa descoberta informa quando suas credenciais de instância são acessadas por uma AWS conta fora do seu AWS ambiente.	20 de janeiro de 2022

Os tipos de descoberta foram atualizados para ajudar a identificar problemas relacionados ao log4j	GuardDuty A Amazon atualizou os seguintes tipos de descoberta para ajudar a identificar e priorizar problemas relacionados a CVE-2021-44228 e CVE-2021-45046:Backdoor:EC2/C&CActivity.B;;Backdoor:EC2/C&CActivity.B!DNS. Behavior:EC2/NetworkPortUnusual	22 de dezembro de 2021
Alterações em descobertas	UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration foi alterado para UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS. Essa versão aprimorada da descoberta aprende os locais típicos em que suas credenciais são usadas para reduzir as descobertas do tráfego roteado por meio de redes locais. UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS	7 de setembro de 2021
Atualização para GuardDuty SLR	A GuardDuty SLR foi atualizada com novas ações para melhorar a precisão da localização.	3 de agosto de 2021

Foram adicionadas informações da fonte de dados para cada tipo de descoberta.	As descrições das descobertas agora contêm informações sobre as fontes de dados GuardDuty usadas para gerar essa descoberta.	10 de maio de 2021
Retirados 13 tipos de descobertas.	13 descobertas foram retiradas para serem substituídas por novas Anomalous Behavoir descobertas. Persistence:IAMUser/NetworkPermissions, Persistence:IAMUser/ResourcePermissions, Persistence:IAMUser/UserPermissionsPrivilegeEscalation:IAMUser/AdministrativePermissions, Recon:IAMUser/NetworkPermissions, Recon:IAMUser/ResourcePermissions, Recon:IAMUser/UserPermissions, ResourceConsumption:IAMUser/ComputeResources, Stealth:IAMUser/LoggingConfigurationModified, Discovery:S3/BucketEnumeration.UnusualImpact:S3/ObjectDelete.Unusual, Impact:S3/PermissionsModification.Unusual,, UnauthorizedAccess:IAMUser/ConsoleLogine.	12 de março de 2021

Foram adicionados 8 novos tipos de descoberta para comportamento anômalo.	Foram adicionados 8 novos tipos de descoberta IAMUser com base no comportamento anômalo dos diretores do IAM. CredentialAccess:IAMUser/AnomalousBehavior, DefenseEvasion:IAMUser/AnomalousBehavior, Discovery:IAMUser/AnomalousBehavior, Exfiltration:IAMUser/AnomalousBehavior, Impact:IAMUser/AnomalousBehavior, InitialAccess:IAMUser/AnomalousBehavior, Persistence:IAMUser/AnomalousBehavior, PrivilegeEscalation:IAMUser/AnomalousBehavior.	12 de março de 2021
Foram adicionadas descobertas do EC2 com base na reputação do domínio.	Foram adicionados 4 novos tipos de descoberta de impacto com base na reputação do domínio. Impact:EC2/AbusedDomainRequest.Reputation , Impact:EC2/BitcoinDomainRequest.Reputation, Impact:EC2/MaliciousDomainRequest.Reputation. Também foi adicionada uma nova descoberta do EC2 para C&CActivity. Impact:EC2/SuspiciousDomainRequest.Reputation	27 de janeiro de 2021

Foram adicionados 4 novos tipos de descoberta.	Foram adicionadas 3 novas descobertas do S3 Malicious IPCaller. Discovery:S3/MaliciousIPCaller, Exfiltration:S3/MaliciousIPCaller, Impact:S3/MaliciousIPCaller. Também foi adicionada uma nova descoberta do EC2 para C&CActivity. Backdoor:EC2/C&CActivity.B	21 de dezembro de 2020
Retirou o tipo de descoberta UnauthorizedAccess:EC2/TorIPCaller.	O tipo de UnauthorizedAccess:EC2/TorIPCaller descoberta agora foi retirado do GuardDuty. Saiba mais.	1.º de outubro de 2020
Foi adicionado o tipo de descoberta Impact:EC2/WinRmBruteForce.	Foi adicionada uma nova descoberta de impacto, Impact:EC2/WinRmBruteForce. Saiba mais.	17 de setembro de 2020
Foi adicionado o tipo de descoberta Impact:EC2/PortSweep.	Foi adicionada uma nova descoberta de impacto, Impact:EC2/PortSweep. Saiba mais.	17 de setembro de 2020
GuardDuty agora está disponível nas regiões da África (Cidade do Cabo) e Europa (Milão).	Foram adicionadas África (Cidade do Cabo) e Europa (Milão) à lista de AWS regiões nas quais GuardDuty está disponível. Saiba mais	31 de julho de 2020

Foram adicionados novos detalhes de uso para monitorar GuardDuty os custos.	Agora você pode usar novas métricas para consultar dados de custo de GuardDuty uso da sua conta e das contas que você gerencia. Uma nova visão geral dos custos de uso está disponível no console em https://console.aws.amazon.com/guardduty/. Informações mais detalhadas podem ser acessadas por meio da API.	31 de julho de 2020
Conteúdo adicionado cobrindo a proteção do S3 por meio do monitoramento de eventos de dados do S3 em. GuardDuty	GuardDuty O S3 Protection agora está disponível por meio do monitoramento de eventos do plano de dados do S3 como uma nova fonte de dados. Novas contas terão esse recurso habilitado automaticamente. Se você já estiver usando, GuardDuty poderá habilitar a nova fonte de dados para você ou para suas contas de membros.	31 de julho de 2020
Foram adicionadas 14 novas descobertas do S3.	Foram adicionados 14 novos tipos de descoberta do S3 ao ambiente de gerenciamento do S3 e às fontes do plano de dados.	31 de julho de 2020

Adição de suporte para descobertas do S3 e alteração de dois nomes de tipos de descobertas existentes.	GuardDuty as descobertas agora incluem mais detalhes sobre descobertas envolvendo buckets S3. Os tipos de descoberta existentes relacionados à atividade do S3 foram renomeados: Policy:IAMUser/S3BlockPublicAccessDisabled foi alterado para Policy:S3/BucketBlockPublicAccessDisabled. Stealth:IAMUser/S3ServerAccessLoggingDisabled foi alterado para Stealth:S3/ServerAccessLoggingDisabled.	28 de maio de 2020
Conteúdo adicionado para AWS Organizations integração.	GuardDuty agora se integra com administradores AWS Organizations delegados para permitir que você gerencie GuardDuty contas em sua organização. Ao definir um administrador delegado como sua conta de GuardDuty administrador, você pode habilitar GuardDuty automaticamente que qualquer membro da organização seja gerenciado pela conta de administrador delegado. Você também pode ativar GuardDuty automaticamente novas contas de AWS Organizations membros. Saiba mais.	20 de abril de 2020

Adição de conteúdo ao recurso Exportar descobertas.	Conteúdo adicionado que descreve o recurso Export Fachts do GuardDuty.	14 de novembro de 2019
Foi adicionado o tipo de descoberta UnauthorizedAccess:EC2/MetadataDNSRebind.	Foi adicionada uma nova descoberta não autorizada, UnauthorizedAccess:EC2/MetadataDNSRebind. Saiba mais.	10 de outubro de 2019
Foi adicionado o tipo de descoberta Stealth:IAMUser/S3ServerAccessLoggingDisabled.	Foi adicionada uma nova descoberta de Stealth, Stealth:IAMUser/S3ServerAccessLoggingDisabled. Saiba mais.	10 de outubro de 2019
Foi adicionado o tipo de descoberta Policy:IAMUser/S3BlockPublicAccessDisabled.	Foi adicionada uma nova descoberta de política, Policy:IAMUser/S3BlockPublicAccessDisabled. Saiba mais.	10 de outubro de 2019
Retirou o tipo de descoberta Backdoor:EC2/XORDDOS.	O tipo de Backdoor:EC2/XORDDOS descoberta agora foi retirado do GuardDuty. Saiba mais	12 de junho de 2019
Foi adicionado o tipo de descoberta PrivilegeEscalation.	O tipo de descoberta Privilege Escalation detecta quando os usuários tentam atribuir privilégios elevados e mais permissivos às suas contas. Saiba mais	14 de maio de 2019
GuardDuty agora está disponível na região da Europa (Estocolmo).	A Europa (Estocolmo) foi adicionada à lista de AWS regiões nas quais GuardDuty está disponível. Saiba mais	9 de maio de 2019

Foi adicionado um novo tipo de descoberta, Recon:EC2/PortProbeEMRUnprotectedPort.	Essa descoberta informa que uma porta EMR-related confidencial em uma instância do EC2 não está bloqueada e está sendo ativamente testada. Saiba mais	8 de maio de 2019
Adicionados 5 novos tipos de descobertas que detectam se as suas instâncias do EC2 podem estar sendo usadas para ataques de negação de serviço (DoS).	Essas descobertas informam as instâncias do EC2 em seu ambiente que estão se comportando de uma forma que pode indicar que estão sendo usadas para executar ataques de negação de serviço (DoS). Saiba mais	8 de março de 2019
Foi adicionado um novo tipo de descoberta: Policy:IAMUser/RootCredentialUsage	Policy:IAMUser/RootCredentialUsagefinding type informa que suas credenciais de login do usuário root Conta da AWS estão sendo usadas para fazer solicitações programáticas aos serviços. AWS Saiba mais	24 de janeiro de 2019
O tipo de descoberta UnauthorizedAccess:IAMUser/UnusualASNCaller foi retirado	O tipo de descoberta UnauthorizedAccess:IAMUser/UnusualASNCaller foi retirado. Agora você será notificado sobre atividades invocadas de redes incomuns por meio de outros tipos de GuardDuty descoberta ativa. O tipo de descoberta gerado será baseado na categoria da API que foi invocada a partir de uma rede incomum. Saiba mais	21 de dezembro de 2018

Foram adicionados dois novos tipos de descoberta: PenTest:IAMUser/ParrotLinux e PenTest:IAMUser/PentooLinux	O tipo de descoberta PenTest:IAMUser/ParrotLinux informa que um computador executando o Parrot Security Linux está fazendo chamadas de API usando credenciais que pertencem à sua conta da AWS . O tipo de descoberta PenTest:IAMUser/PentooLinux informa que uma máquina executando o Pentoo Linux está fazendo chamadas de API usando credenciais que pertencem à sua conta da AWS . Saiba mais	21 de dezembro de 2018
Foi adicionado suporte para o tópico SNS de GuardDuty anúncios da Amazon	Agora você pode se inscrever no tópico de GuardDuty anúncios do SNS para receber notificações sobre tipos de descoberta recém-lançados, atualizações dos tipos de descoberta existentes e outras alterações de funcionalidade. As notificações estão disponíveis em todos os formatos compatíveis com o Amazon SNS. Saiba mais	21 de novembro de 2018

Foram adicionados dois novos tipos de descoberta: UnauthorizedAccess:EC2/TorClient e UnauthorizedAccess:EC2/TorRelay	UnauthorizedAccess:EC2/TorClientfinding type informa que uma instância do EC2 em seu AWS ambiente está fazendo conexões com um nó Tor Guard ou Authority . UnauthorizedAccess:EC2/TorRelayfinding type informa que uma instância do EC2 em seu AWS ambiente está fazendo conexões com uma rede Tor de uma maneira que sugere que ela está agindo como um retransmissor Tor. Saiba mais	16 de novembro de 2018
Foi adicionado um novo tipo de descoberta: CryptoCurrency:EC2/BitcoinTool.B	Essa descoberta informa que uma instância do EC2 em seu AWS ambiente está consultando um nome de domínio associado ao Bitcoin ou a outra atividade relacionada à criptomoeda. Saiba mais	9 de novembro de 2018
Foi adicionado suporte para atualizar a frequência das notificações enviadas para CloudWatch Eventos	Agora você pode atualizar a frequência das notificações enviadas aos CloudWatch Eventos para as ocorrências subsequentes das descobertas existentes. Valores possíveis são 15 minutos, 1 hora ou 6 horas (padrão). Saiba mais	9 de outubro de 2018
Adição de suporte à região	Suporte regional adicionado para AWS GovCloud (US-West) Saiba mais	25 de julho de 2018

Suporte adicionado para CloudFormation StackSets em GuardDuty	Você pode usar o GuardDuty modelo Enable Amazon para habilitar GuardDuty simultane amente em várias contas. Saiba mais	25 de junho de 2018
Foi adicionado suporte para regras de GuardDuty arquivamento automático	Agora, os clientes podem criar regras de autoarqui vamento granulares para a supressão de descobert as. Para descobertas que correspondam a uma regra de arquivamento automátic o, marque-as GuardDuty automaticamente como arquivadas. Isso permite que os clientes se ajustem ainda mais GuardDuty para manter apenas as descobert as relevantes na tabela de descobertas atual. Saiba mais	4 de maio de 2018
GuardDuty está disponível na região Europa (Paris)	GuardDuty agora está disponível na Europa (Paris), permitindo que você amplie o monitoramento contínuo da segurança e a detecção de ameaças nessa região. Saiba mais	29 de março de 2018
Agora CloudFormation é GuardDuty possível criar contas de administrador e contas de membros por meio de.	Para obter mais informaçõ es, consulte `AWS::GuardDuty::master` e `AWS::GuardDuty::member`.	6 de março de 2018

Foram adicionadas nove novas detecções de CloudTrail-based anomalias.	Esses novos tipos de descoberta são habilitados automaticamente GuardDuty em todas as regiões suportadas. Saiba mais	28 de fevereiro de 2018
Foram adicionadas três novas detecções de inteligência de ameaças (tipos de descoberta).	Esses novos tipos de descoberta são habilitados automaticamente GuardDuty em todas as regiões suportadas. Saiba mais	5 de fevereiro de 2018
Aumento do limite para contas de GuardDuty membros.	Com esta versão, você pode ter até 1000 contas de GuardDuty membros adicionadas por AWS conta (conta de GuardDuty administrador). Saiba mais	25 de janeiro de 2018
Mudanças no upload e no gerenciamento adicional de listas de IP confiáveis e listas de ameaças para contas de GuardDuty administrador e contas de membros.	Com esta versão, os usuários de GuardDuty contas de administrador podem carregar e gerenciar listas de IP confiáveis e listas de ameaças. Usuários de GuardDuty contas de membros não podem fazer upload e gerenciar listas. As listas de IP confiáveis e as listas de ameaças enviadas pela conta do administrador são impostas à GuardDuty funcionalidade de suas contas de membros. Saiba mais	25 de janeiro de 2018

Atualizações anteriores

Alteração	Descrição	Data
Publicação inicial	Publicação inicial do Guia GuardDuty do usuário da Amazon.	28 de novembro de 2017

As traduções são geradas por tradução automática. Em caso de conflito entre o conteúdo da tradução e da versão original em inglês, a versão em inglês prevalecerá.