



Manual do usuário

AWS Gerenciamento de contas



AWS Gerenciamento de contas: Manual do usuário

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 desprestige 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 um Conta da AWS?	1
Características de um Conta da AWS	3
Você é a primeira vez? AWS usuário?	3
Suporte e feedback	4
Outros AWS recursos	4
Compare as opções de inscrição	6
Compatível Serviços da AWS para Inscreva-se em AWS (novo)	6
Serviços da AWS incluído no nível gratuito do nosso novo AWS experiência	7
Serviços da AWS incluído no plano pago do nosso novo AWS experiência	12
Serviços da AWS não é compatível com nosso novo AWS experiência	13
Considerações sobre como escolher como se inscrever no AWS	18
Compare os recursos das opções de inscrição	19
Compare o gerenciamento de acesso	20
Gerencie seu Contas da AWS	22
Inscreva-se para AWS (novo)	26
Inscreva-se usando Inscrever-se em AWS (novo)	28
Próximas etapas	29
AWS Configurações de uso	30
Conecte uma ferramenta de codificação de IA	31
Considerações para conectar sua ferramenta de codificação ao seu projeto	31
Conecte sua ferramenta de codificação de IA ao seu projeto	32
Trabalhe com vários projetos	33
AWS ações para proprietários de projetos	35
Atualize sua senha	36
Gerencie a autenticação multifator (MFA)	37
Principais pontos	37
Tipos de MFA disponíveis para nosso novo AWS experiência	38
Registrar seu dispositivo de MFA do	40
Registrar uma chave de segurança como seu dispositivo de MFA do	41
Renomear seu dispositivo de MFA do	42
Exclua seu dispositivo de MFA	42
Excluir todas as sessões	43
Gerencie seu nome ou apelido	44
Alterar seu endereço de e-mail	45

Editar suas informações de contato	45
Optar por não usar seu conteúdo para melhorar o serviço	46
Solicite seus dados de AWS Builder ID	47
Criar um projeto	48
Considerações para criar um projeto	48
Para criar um projeto	49
Regiões da AWS para seus projetos	50
Encontre o selecionado Região da AWS para seus projetos	51
Países onde os recursos regionais são provisionados no Leste dos EUA (Ohio) (us-east-2)	51
Países onde os recursos regionais são provisionados na Ásia-Pacífico (Sydney) (ap-southeast-2)	54
Países onde os recursos regionais são provisionados na Europa (Estocolmo) (eu-north-1)	57
Políticas gerenciadas para sua organização	64
Políticas de controle de serviços para projetos	64
Políticas de controle de serviço para o nível gratuito para projetos	86
Políticas de controle de serviço para o plano pago para projetos	97
Políticas de controle de recursos para projetos	109
Alternar entre projetos	111
Alternar entre projetos para sessões ativas a partir do Console de gerenciamento da AWS	111
Alternar entre projetos em AWS Configurações	112
Alternar entre projetos a partir do Console de gerenciamento da AWS	112
Convide membros da equipe	112
Considerações para os membros da equipe	113
Como os membros da equipe acessam seu AWS recursos	114
Convide membros da equipe	115
Convide um membro da equipe para um projeto	115
Remover um membro da equipe de um projeto	116
Remover um membro da equipe	117
Revogar um convite	117
Reenviar um convite	118
Atualize sua conta	119
Considerações para atualizar sua conta	119
Atualize sua conta	120

Criar um limite de gastos	120
O que é um limite de gastos?	120
Defina seu limite de gastos	121
Notificações	122
Personalize suas configurações de limite de gastos com controles de custo antecipados opcionais	122
O que acontece se você atingir seu limite	123
Outras coisas importantes a serem observadas	124
Crie um limite de gastos em AWS Configurações	124
Atualizar um limite de gastos	125
Atualizar um limite de gastos em AWS Configurações	125
Remover um limite de gastos	126
Remova um limite de gastos em AWS Configurações	126
Nível gratuito	126
Acompanhar seu uso do nível gratuito	127
Ganhe créditos adicionais	129
Visualize suas informações de cobrança em AWS Configurações	129
Para ver seu custo por projeto	130
Visualize seu histórico de cobrança em AWS Configurações	130
Gerencie seu método de pagamento	131
Faça um pagamento em AWS Configurações	132
Altere sua moeda preferida em AWS Configurações	132
Gerencie o registro fiscal em AWS Configurações	133
Como atualizar e excluir números de registro fiscal	133
Gerenciar suas isenções fiscais nos EUA	134
Exibir e resgatar créditos	135
Gerenciar contas na Índia	136
Cadastre-se para AWS (novo) com AWS Índia	136
Gerenciar suas informações de verificação do cliente	138
Configure seu faturamento na Índia	142
Adicionar ou editar um número de conta permanente (PAN)	142
Editar vários números de conta permanente	143
Editar vários números de impostos sobre bens e serviços	143
Visualizar uma fatura fiscal	144
Alterando o vendedor do registro de ou para AWS Índia	144
Acesse o AWS Support	146

Apoio ao projeto	146
Technical support (Suporte técnico)	147
Support se todos os seus projetos e organização estiverem fechados	148
Inicie um teste do Business Support+	148
Monitore seu projeto	149
Monitore seu projeto usando AWS CloudTrail	149
Use CloudTrail para ver quem modificou seu projeto	149
Fechar um projeto	152
O que você precisa saber antes de fechar seu projeto	152
Para fechar um projeto	153
Post-closure período	154
Reabrindo seu projeto	154
Ative recursos avançados	154
O que acontece quando você ativa recursos avançados	155
Contas do projeto depois de ativar os recursos avançados	157
Como será AWS As configurações mudam depois que eu ativo os recursos avançados?	158
Ainda posso criar um projeto no AWS Configurações após eu ativar os recursos avançados?	159
Como se preparar para ativar recursos avançados	160
Como ativar recursos avançados	160
Depois de ativar os recursos avançados	161
Definir uma senha de usuário root	162
Gerencie membros da força de trabalho	163
Alterar fonte de identidade	165
Remover políticas da organização	166
Feche sua conta em AWS Configurações	168
O que você precisa saber antes de fechar sua conta de gerenciamento	168
Fechar um projeto	169
Feche sua conta de gerenciamento	169
Exclua seu AWS ID do builder	169
Inscreva-se para AWS (avançado)	171
Etapa 1: criar a conta	172
Etapa 2: (recomendado) instalar o AWS CLI	174
Etapa 3: (Recomendado) Configurar o AWS Servidor MCP	175
Relacionado AWS serviços	175
Uso do usuário-raiz	177

Como acessar a conta	177
Planejar a estrutura de governança	178
Benefícios do uso de vários Contas da AWS	179
Quando usar AWS Organizations	181
Quando usar AWS Control Tower	187
Noções básicas dos modos de operação da API	188
Configurar a conta	192
Criar ou atualizar o alias da conta	192
Ativar ou desativar Regiões da AWS na sua conta	193
Atualize o faturamento do seu Conta da AWS	204
Atualize o e-mail do usuário-raiz	204
Atualizar senha do usuário-raiz	210
Atualize seu Conta da AWS name	211
Atualize os contatos alternativos para seu Conta da AWS	215
Atualize o contato principal do seu Conta da AWS	224
Visualizar os identificadores da conta	235
Solucionar problemas da conta	241
Problemas de criação da conta	241
Problemas com encerramento da conta	242
Outros problemas	244
Gerenciar contas na Índia	245
Crie um Conta da AWS por AWS Índia	246
Gerenciar suas informações de verificação do cliente	248
Encerrar a conta	254
O que você precisa saber antes de encerrar a conta	254
Como encerrar uma conta	257
O que esperar depois de encerrar a conta	260
Reabra sua conta	261
O que você precisa saber antes de reabrir sua conta	261
Como reabrir sua conta	262
O que esperar depois de reabrir sua conta	263
Prepare sua conta para uso após a reabertura	263
Disponibilidade de regiões	263
Proteger a conta	264
Proteção de dados	265
AWS PrivateLink	266

Criação do endpoint	266
Políticas de endpoint da Amazon VPC	267
Políticas de endpoint	267
Gerenciamento de Identidade e Acesso	268
Público	269
Autenticação com identidades	269
Gerenciar o acesso usando políticas	270
AWS Gerenciamento de contas e IAM	272
Identity-based exemplos de políticas	280
Usar políticas baseadas em identidade	284
Solução de problemas	287
AWS políticas gerenciadas	289
AWSAccountManagementReadOnlyAccess	290
AWSAccountManagementFullAccess	291
Atualizações da política	292
Validação de conformidade	293
Resiliência	294
Segurança da infraestrutura	294
Monitorar a conta	296
CloudTrail troncos	296
Informações de gerenciamento de contas em CloudTrail	297
Noções básicas das entradas de log do Gerenciamento de Contas	298
Monitorando eventos de gerenciamento de contas com EventBridge	301
Eventos do Gerenciamento de Contas	302
Cotas	305
Histórico do documento	308
.....	cccxix

O que é um Conta da AWS?

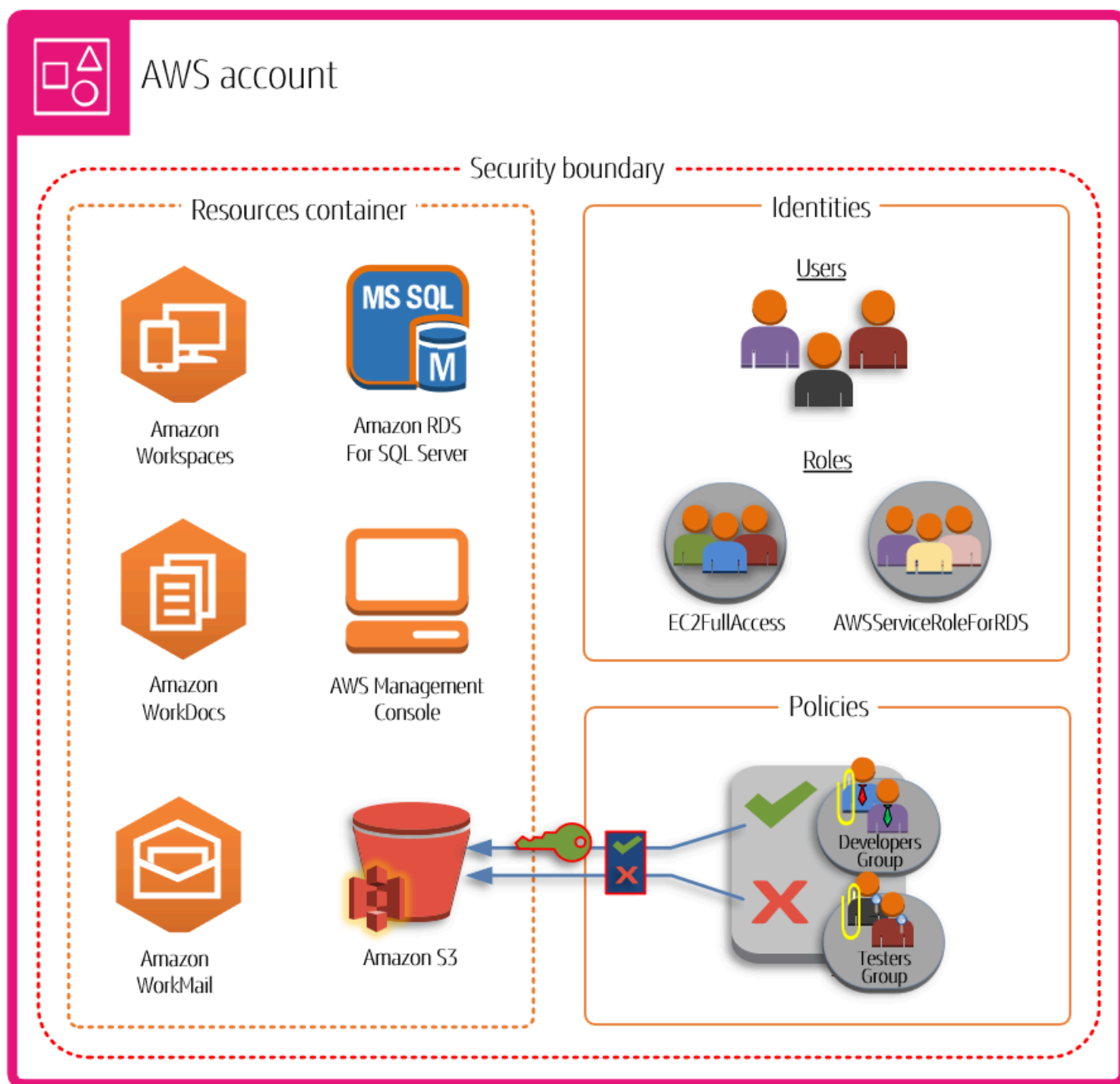
An Conta da AWS representa uma relação comercial formal com a qual você estabelece AWS. Você cria e gerencia seus AWS recursos em um Conta da AWS, e sua conta fornece recursos de gerenciamento de identidade para acesso e cobrança. Cada um Conta da AWS tem um ID exclusivo que o diferencia dos outros Contas da AWS.

Ao se inscrever AWS, você pode escolher entre Inscrever-se em AWS (novo) e Inscrever-se em AWS (avançado). Dependendo da sua escolha, você tem acesso aos Contas da AWS nossos projetos. Os projetos contêm Contas da AWS e as configurações para compartilhar com outros colaboradores. Para obter mais informações, consulte [Compare as opções de inscrição](#).

Seus recursos e dados na nuvem estão contidos em uma Conta da AWS. Uma conta atua como um limite de isolamento do gerenciamento de identidade e acesso. Quando precisar compartilhar recursos e dados entre duas contas, você deverá explicitamente permitir esse acesso. Por padrão, nenhum acesso é permitido entre contas. Por exemplo, se você designar contas diferentes para conter seus recursos e dados de produção e não produção, nenhum acesso será permitido entre esses ambientes, por padrão.

Contas da AWS também são uma parte fundamental do acesso aos AWS serviços. Conforme mostrado na ilustração a seguir, um Conta da AWS tem duas funções principais:

- **Contêiner de recursos** — Um Conta da AWS é o contêiner básico para todos os AWS recursos que você cria como AWS cliente. Por exemplo, um bucket do Amazon Simple Storage Service (Amazon S3), um banco de dados do Amazon Relational Database Service (Amazon RDS) e uma instância do Amazon Elastic Compute Cloud (Amazon EC2) são todos recursos. Cada recurso é identificado exclusivamente por um nome do recurso da Amazon (ARN) que inclui o ID da conta que contém ou possui o recurso.
- **Limite de segurança** — An também Conta da AWS é o limite básico de segurança para seus AWS recursos. Os recursos que você cria na conta estão disponíveis para os usuários que têm credenciais desta conta. Entre os principais recursos que você pode criar na conta estão as identidades, como usuários e perfis. Essas identidades têm credenciais que alguém pode usar para fazer login (ou autenticar-se) na AWS. As identidades também têm políticas de permissão que especificam o que um usuário pode fazer (autorização) com os recursos da conta.



Usar várias Contas da AWS é a melhor prática para escalar seu ambiente, pois fornece um limite natural de faturamento para os custos, isola recursos para garantir a segurança, oferece flexibilidade para indivíduos e equipes, além de ser adaptável a novos processos de negócios. Para obter mais informações, consulte [Benefícios do uso de várias Contas da AWS](#).

Características de um Conta da AWS

Contas da AWS incluem os seguintes recursos principais:

- **Monitore e controle os custos** — Uma conta é o meio padrão pelo qual AWS os custos são alocados. Por esse motivo, o uso de contas diferentes para diferentes unidades de negócios e grupos de workloads pode ajudar você a rastrear, controlar, prever, orçar e relatar com mais facilidade suas despesas com a nuvem. Além dos relatórios de custos no nível da conta, AWS também tem suporte integrado para consolidar e relatar custos em todo o conjunto de contas, caso você opte por usar AWS Organizations em algum momento. Você também pode usar o AWS Service Quotas para ajudar na proteção contra o provisionamento excessivo inesperado de recursos da AWS e de ações mal-intencionadas que podem afetar drasticamente os custos da AWS.
- **Unidade de isolamento** — An Conta da AWS fornece limites de segurança, acesso e cobrança para seus AWS recursos que podem ajudá-lo a obter autonomia e isolamento de recursos. Por design, todos os recursos provisionados em uma conta são logicamente isolados dos recursos provisionados em outras contas, mesmo em seu próprio ambiente. AWS Esse limite de isolamento fornece uma maneira de limitar os riscos de um problema relacionado à aplicação, a uma configuração incorreta ou a ações mal-intencionadas. Se ocorrer um problema em uma conta, os impactos nas workloads contidas em outras contas poderão ser reduzidos ou eliminados.
- **Espelhar workloads de negócios**: use várias contas para agrupar workloads com um objetivo comum de negócios em contas distintas. Como resultado, você pode alinhar a propriedade e a tomada de decisões com essas contas e evitar dependências e conflitos com a forma como as workloads de outras contas são protegidas e gerenciadas. Dependendo do seu modelo geral de negócios, você pode optar por isolar unidades de negócios ou subsidiárias distintas em contas diferentes. Essa abordagem também pode facilitar a alienação dessas unidades ao longo do tempo.

Você é a primeira vez? AWS usuário?

Warning

No momento, estamos lançando nossa nova experiência para um número limitado de clientes. Talvez você ainda não consiga acessar essa experiência.

Se você é usuário iniciante do AWS, sua primeira etapa é se inscrever AWS no. Você pode criar um Conta da AWS em que tenha controle total sobre a configuração da conta e onde seu conteúdo é armazenado, o que é necessário para cargas de trabalho regulamentadas, como HIPAA ou FedRAMP, ou criar com padrões pré-configurados. Contas da AWS Para saber qual inscrição é ideal para você, consulte [Compare as opções de inscrição](#).

Para obter instruções detalhadas sobre como configurar uma nova conta na qual você tenha controle total sobre a configuração inicial, consulte. [Inscreva-se para AWS \(avançado\)](#)

Para obter instruções detalhadas sobre como configurar uma nova conta onde AWS cria contas com padrões pré-configurados, consulte. [Inscreva-se para AWS \(novo\)](#)

Suporte para AWS Gerenciamento de contas

Você pode publicar feedback e perguntas usando o [AWS Account Management support forum](#). Para obter informações gerais sobre AWS fóruns, consulte [AWS re:Post](#).

Se não conseguir encontrar as respostas que está procurando AWS re:Post, você pode criar um caso de suporte relacionado à conta ou cobrança usando o Console de gerenciamento da AWS. Para obter mais informações, consulte [Example: Create a support case for account and billing](#).

Outros AWS recursos

- [AWS Treinamento e cursos](#) — Links para cursos especializados e baseados em funções, bem como laboratórios individualizados para ajudar a aprimorar suas AWS habilidades e ganhar experiência prática.
- [AWS Ferramentas para desenvolvedores](#) — Links para ferramentas e recursos para desenvolvedores que fornecem documentação, exemplos de código, notas de versão e outras informações para ajudá-lo a criar aplicativos inovadores AWS.
- [AWS Support Center](#) — O hub para criar e gerenciar seus casos de AWS Support. Também inclui links para outros recursos úteis, como fóruns, perguntas frequentes, status de integridade do serviço e AWS Trusted Advisor.
- [AWS Support](#) — A principal página da web com informações sobre o AWS Support, um canal de suporte individual e de resposta rápida para ajudá-lo a criar e executar aplicativos na nuvem.
- [Fale conosco](#) — Um ponto de contato central para consultas sobre AWS faturamento, conta, eventos, abuso e outros problemas.

- [AWS Termos do site](#) — Informações detalhadas sobre nossos direitos autorais e nossa marca registrada; sua conta, licença e acesso ao site; e outros tópicos.

Compare as opções de inscrição

Warning

No momento, estamos lançando nossa nova experiência para um número limitado de clientes. Talvez você ainda não consiga acessar essa experiência.

Ao se inscrever AWS, você desbloqueia a nuvem mais abrangente e amplamente adotada do mundo. Oferecemos a melhor opção de recursos e experiência inovadores em nuvem e IA, na mais ampla infraestrutura global, com segurança, confiabilidade e desempenho líderes do setor.

Há duas maneiras de se inscrever em AWS. Se você quiser controle total sobre a configuração da conta e onde seu conteúdo é armazenado, ou se você tiver cargas de trabalho regulamentadas, como HIPAA, FedRAMP, use. [Inscreva-se para AWS \(avançado\)](#) Se você for um novo usuário e quiser usar um login que já possui para entrar AWS e criar um AWS ambiente com padrões pré-configurados em select [Regiões da AWS](#), use. [Inscreva-se para AWS \(novo\)](#)

Compatível Serviços da AWS para Inscreva-se em AWS (novo)

Warning

No momento, estamos lançando nossa nova experiência para um número limitado de clientes. Talvez você ainda não consiga acessar essa experiência.

Ao usar Inscrever-se em AWS (novo), você tem acesso ao nível gratuito. O nível gratuito fornece acesso a AWS serviços selecionados. Você pode atualizar sua conta para um plano pago para acessar AWS serviços e recursos adicionais. Para saber como atualizar sua conta, consulte [Atualize sua conta em AWS Configurações](#).

Nem todo AWS serviço está disponível para Inscrever-se em AWS (novo). Se um serviço não estiver listado em nenhuma das listas a seguir ou tiver um recurso não suportado, você deverá criar uma conta usando [Inscreva-se para AWS \(avançado\)](#) ou [Ativar avançado AWS recursos](#).

Serviços da AWS incluído no nível gratuito do nosso novo AWS experiência

Os AWS serviços a seguir estão incluídos no nível gratuito de inscrição AWS (novo). Multi-Region ou Os recursos entre regiões não são compatíveis com nenhum serviço. Para obter mais informações, consulte [Regiões da AWS para seus projetos](#).

- Amazon API Gateway
- Amazon Athena
- Amazon AppFlow
- AWS App2Container
- Amazon Augmented AI
- Amazon Bedrock
- Amazon Bedrock Agent Core
- Amazon CloudFront
 - O Lambda @Edge não é compatível.
- Amazon CloudWatch
- CloudWatch Registros da Amazon
- Amazon CodeGuru Profiler
- Amazon Cognito
- Amazon Cognito Sync
- Amazon DynamoDB
- Amazon DataZone
- Amazon Elastic Container Registry (ECR)
- EC2 Image Builder
- Amazon EKS Anywhere
- Amazon Elastic Block Store (EBS)
- Amazon Elastic Compute Cloud (EC2)
 - O Bloco de Capacidade de Compra e a Extensão de Bloco de Capacidade de Compra não são suportados.
- Amazon Elastic Container Registry Public
- Amazon Elastic Container Service

- Amazon Elastic Kubernetes Service
- Amazon Elastic File System
- Amazon ElastiCache
- Amazon EventBridge
- Amazon Lex
- Amazon Lightsail
- Amazon Location Service
- Amazon Managed Service for Prometheus
- Amazon Managed Workflows for Apache Airflow
- Amazon MQ
- OpenSearch Serviço Amazon
- Amazon Polly
- Amazon Quick
 - Somente o Amazon Quick Free ou o Quick Plus são suportados. Para obter mais informações, consulte os [preços do Amazon Quick](#).
- Amazon Rekognition
- Amazon Relational Database Service
- Amazon Route 53
- Amazon SageMaker
- SageMaker IA da Amazon
- Amazon SageMaker Unified Studio
- Amazon Simple Email Service
- Amazon Simple Notification Service
- Amazon Simple Queue Service
- Amazon Simple Storage Service
 - O Amazon S3 Access Grants não é suportado.
- Amazon Simple Workflow Service
- Amazon Verified Permissions
- Amazon Virtual Private Cloud

- Amazon Aurora
- Amazon Aurora DSQL
- AWS Amplify
- AWS AppConfig
- AWS AppSync
- Application Auto Scaling
- AWS Transform MGN
- AWS Artifact
 - O Adendo de Associado AWS Comercial (HIPAA), o Adendo de Associado Comercial de AWS Organizações (HIPAA), o Adendo da Regra 17a-4 da SEC e o Adendo da Regra 18a-6 da AWS SEC não são suportados. AWS
- AWS B2B Data Interchange
- Agente do AWS Backint
- AWS Backup
- AWS Batch
- Gerenciamento de Faturamento e Custos da AWS
 - Use AWS as Configurações para configurar seu faturamento, criar limites de gastos para controlar seus custos e recuperar e pagar faturas. Você usa o Billing and Cost Management para criar orçamentos, analisar e otimizar seus custos. Para obter mais informações, consulte [Como usar o console Billing and Cost Management com nossa AWS nova experiência](#).
- AWS Budgets
- Gerenciador de certificados da AWS
 - AWS Não há suporte para [certificados públicos exportáveis do Certificate Manager](#).
- AWS API Cloud Control
- AWS Cloud Map
- AWS Cloud9
- AWS CloudFormation
- AWS CloudShell
- AWS CloudTrail
- AWS CodeArtifact

- AWS CodeCommit
- AWS CodeDeploy
- AWS CodePipeline
- AWS Compute Optimizer
- AWS Config
- AWS Console Mobile Application
- AWS Cost Explorer
- AWS Data Pipeline
- AWS Transferência de dados
- AWS DataSync
- AWS Directory Service
- AWS Elastic Beanstalk
- AWS End User Messaging Social
- AWS Entity Resolution
- AWS Glue
- AWS Health
- AWS Identity and Access Management
- AWS IoT
 - AWS O Greengrass não é suportado.
- AWS IoT Defensor do dispositivo
- AWS IoT Gerenciamento de dispositivos
- AWS IoT SiteWise
- AWS IoT TwinMaker
- AWS Key Management Service
- AWS Lake Formation
- AWS Lambda
 - O Lambda @Edge não é compatível.
- AWS Launch Wizard
- AWS License Manager

- Console de gerenciamento da AWS
- AWS Marketplace
 - Somente Bedrock and Free.
- AWS Network Manager
- AWS Payment Cryptography
- AWS PrivateLink
- AWS Resource Access Manager (RAM)
- Explorador de recursos da AWS
- Grupos de recursos da AWS
- Controlador de recuperação de aplicativos (ARC) da Amazon Route 53
- AWS SDKs e ferramentas
- AWS Secrets Manager
- AWS Security Token Service
- AWS Serverless Application Repository
- Service Quotas
- AWS Signer
- AWS Step Functions
- AWS Support
- AWS Systems Manager
- AWS Systems Manager para SAP
- Notificações de Usuários da AWS
 - User-configured notificações e operações de configuração de notificações gerenciadas não são suportadas. Para obter mais informações, consulte [O que são notificações AWS do usuário?](#)
- AWS WAF
 - AWS O Shield não é suportado.
- AWS Well-Architected Tool
- AWS X-Ray
- AWS CodeBuild
- Elastic Load Balancing

- AWS SQL Workbench
- Amazon OpenSearch Service sem servidor
- Amazon Timestream

Para ver a política que controla o acesso aos serviços de nível gratuito, consulte [Políticas de controle de serviço para o nível gratuito para projetos](#).

Serviços da AWS incluído no plano pago do nosso novo AWS experiência

Os serviços a seguir estão disponíveis para inscrição AWS (novo) se você tiver um plano pago. Para obter mais informações, consulte [Atualize sua conta em AWS Configurações](#). Multi-Region ou Os recursos entre regiões não são compatíveis com nenhum serviço. Para obter mais informações, consulte [Regiões da AWS para seus projetos](#).

- DevOpsGuru da Amazon
- Amazon DocumentDB (compatível com MongoDB)
- Amazon EMR
- Amazon Forecast
- Amazon Glacier
- Amazon Kinesis
- Amazon Kinesis Data Streams
- Amazon Data Firehose
- Amazon Kinesis Video Streams
- Amazon Managed Blockchain
- Amazon Managed Streaming for Apache Kafka
- Amazon MemoryDB
- Amazon Neptune
- Amazon Personalize
- banco de dados de origem
- S3 Glacier Deep Archive
- Amazon Textract
- Amazon Transcribe

- Amazon Translate
- AWS AppFabric
- AWS Data Exchange
- AWS End User Messaging SMS
- AWS Fault Injection Service
- AWS Firewall Manager
- AWS Network Firewall
- AWS Agente de segurança
- AWS Storage Gateway
- DevOps Agente

Para ver a política que controla o acesso aos serviços do Plano Pago, consulte [Políticas de controle de serviço para o plano pago para projetos](#).

Serviços da AWS não é compatível com nosso novo AWS experiência

Os seguintes AWS serviços não são compatíveis com nossa nova AWS experiência, a menos que você [Ativar avançado AWS recursos](#). Esses AWS serviços não são necessários para novos desenvolvedores ou equipes pequenas. Alguns desses serviços são ativados automaticamente em sua conta e gerenciados por AWS. Para obter mais informações, consulte [Compare os recursos das opções de inscrição](#).

- Alexa for Business
- Alexa Top Sites
- Alexa Web Information Service
- Amazon Braket
- Amazon Chime
- Amazon Chime Business Calling, um serviço vendido pela AMCS LLC
- Amazon Chime Ligue para mim
- Amazon Chime Call Me, um serviço vendido pela AMCS LLC
- Amazon Chime Dial In, um serviço vendido pela AMCS LLC
- Amazon Chime Dialin

- Características do Amazon Chime
- SDK do Amazon Chime
- Serviços Amazon Chime
- Amazon Chime SMS
- Amazon Chime Voice Connector, um serviço vendido pela AMCS LLC
- Amazon Cloud Directory
- Amazon CloudSearch
- Amazon CodeWhisperer
- Amazon Connect Customer
- Perfis de clientes do Amazon Connect Customer
- ID de voz do Amazon Connect Customer
- AWS Deadline Cloud
- Amazon Detective
- Amazon Elastic Inference
- Amazon Elastic Transcoder
- Amazon FinSpace
- Frota flexível da Amazon
- Amazon Fraud Detector
- Amazon FSx
- GameLift Servidores Amazon
- Amazon GameLift Streams
- Amazon GameSparks
- Amazon GuardDuty
- AWS HealthOmics
- Amazon Inspector Classic
- Amazon Interactive Video Service
- Chat do Amazon IVS
- Amazon Kendra

- Amazon Keyspaces (para Apache Cassandra)
- Kiro
- Amazon Macie
- Amazon Managed Grafana
- Amazon Mechanical Turk
- Recompensas para trabalhadores do Amazon Mechanical Turk
- Amazon Mobile Analytics
- Amazon Monitron
- Amazon Nimble Studio
- OpenSearch Serviço de ingestão de serviços da Amazon
- Amazon Q
- Amazon Q Business
- Amazon Q Developer
- Amazon Quantum Ledger Database (Amazon QLDB)
- Amazon S3 on Outposts
- Amazon SageMaker Ground Truth
- Amazon Security Lake
- Amazon Sumerian
- Amazon WorkDocs
- Amazon WorkSpaces
- WorkSpaces Instâncias da Amazon
- WorkSpaces Aplicativos da Amazon (WorkSpaces Aplicativos da Amazon)
- Amazon WorkSpaces Thin Client
- Amazon WorkSpaces Web
- Amazon WorkLink
- Amazon WorkMail
- AWS Perfil de custos de aplicativos
- AWS Clean Rooms
- AWS Estúdio de aplicativos

- AWS Application Discovery Service
- AWS Audit Manager
- AWS Billing Conductor
- AWS CloudHSM
- AWS Client VPN
- AWS WAN em nuvem
- AWS Control Tower
- AWS Database Migration Service
- AWS DeepRacer
- AWS Device Farm
- AWS Direct Connect
- Recuperação de desastres do AWS Elastic
- AWS Elemental Live
- AWS Elemental MediaConnect
- AWS Elemental MediaConvert
- AWS Elemental MediaLive
- AWS Elemental MediaPackage
- AWS Elemental MediaStore
- AWS Elemental MediaTailor
- AWS Global Accelerator
- AWS Ground Station
- AWS HealthImaging
- Centro de Identidade do AWS IAM
- AWS Identity and Access Management Access Analyzer
- AWS Interconexão
- AWS IoT Eventos
- AWS IoT FleetWise
- AWS IoT RoboRunner
- AWS Mainframe Modernization

- AWS Migration Hub
- AWS Migration Hub Refactor Spaces
- AWS Modular Data Center
- AWS OpsWorks
- AWS Organizations
- AWS Outposts
- AWS Parallel Computing Service
- AWS Partner Network
- AWS Calculadora de Preços
- Autoridade de certificação privada da AWS
- AWS Proton
- AWS re:Post Privado
- AWS Resilience Hub
- AWS RoboMaker
- AWS Tecido RTB
- AWS Security Hub
- AWS Security Incident Response
- AWS Service Catalog
- AWS Shield
- AWS SimSpace Weaver
- AWS Snowball
- Cadeia de Suprimentos AWS
- AWS Telco Network Builder
- AWS Transform
- AWS Transfer Family
- AWS Transit Gateway
- AWS Trusted Advisor
- Acesso Verificado pela AWS
- Site-to-Site VPN

- Amazon VPC Lattice
- AWS Wickr
- Amazon CodeCatalyst
- Amazon Comprehend Medical
- Telecomunicações de conferência (serviço vendido pela AMCS LLC)
- Contact Center Telecommunications (serviço vendido pela AMCS LLC)
- Contact Center Telecommunications Korea
- Contact Center Telecommunications na África do Sul
- DynamoDB Accelerator
- Amazon Elastic VMware Service
- Oracle Database@AWS
- Serviço Red Hat OpenShift na AWS
- AWS App Runner

Considerações sobre como escolher como se inscrever no AWS

Considere o seguinte antes de escolher seu método de inscrição. Você pode ativar todos os AWS recursos da sua conta, se necessário.

- Se você tiver requisitos específicos do produto, como cargas de trabalho regulamentadas que incluem HIPAA ou FedRAMP, não use nossa nova experiência. AWS
- Seu conteúdo será armazenado em uma região designada, selecionada com base em suas informações de contato.
- A nova AWS experiência torna mais fácil começar a criar sem criar AWS permissões. Se você precisar de um controle refinado sobre seus usuários ou permissões baseadas em funções, não use Inscrever-se em (novo). AWS
- Se você precisar de configurações de pagamento específicas da conta definidas pelo AWS, também conhecido como faturamento com condições líquidas, não use Inscrever-se em (novo). AWS
- Se você precisar acessar o conjunto completo de AWS serviços, não use Inscrever-se em AWS (novo). Para obter mais informações, consulte [Compatível Serviços da AWS para Inscreva-se em AWS \(novo\)](#).

Compare os recursos das opções de inscrição

A tabela a seguir compara os requisitos AWS abrangentes que são compatíveis com o Cadastro AWS (novo) ou o Cadastro no AWS (avançado). Se um recurso não estiver listado nesta tabela ou descrito em [Compare o gerenciamento de acesso](#), ele estará disponível. Você pode ativar recursos avançados para sua conta se precisar de algum dos recursos não suportados. Para obter mais informações, consulte [Ativar avançado AWS recursos](#).

Recurso	Inscreva-se para AWS (novo)	Inscreva-se para AWS (avançado)
Junte-se à rede de AWS parceiros	Não	Sim
Crie um contrato de serviços profissionais	Não	Sim
Inscreva-se em um contrato empresarial com AWS	Não	Sim
Compre uma assinatura do AWS Skill Builder Team	Não	Sim
Trabalhe com um parceiro AWS de treinamento	Não	Sim
Ganhe créditos extras com o AWS Activate	Não	Sim
Use o AWS Marketplace	Não	Sim
Designe sua AWS conta como compatível com HIPAA ou SEC	Não	Sim
Selecione um específico Região da AWS para criar seus recursos regionais	Não. Para obter mais informações, consulte Regiões da AWS para seus projetos .	Sim
Acesse uma região opcional	Não	Sim
IAM Access Analyzer	Não	Sim

Recurso	Inscreve-se para AWS (novo)	Inscreve-se para AWS (avançado)
Sign-in políticas de acesso	Não	Sim
Crie limites de gastos para suas contas	Sim	Não
Savings Plans	Não	Sim
Opção automática pelo Cust Optimization Hub para o plano pago	Sim	Não
Opção automática para AWS Organizations	Sim	Não
Aceitação automática ao IAM Identity Center	Sim	Não
Inscriver-se automaticamente no gerenciador de funções do IAM	Sim	Não
Cores da conta do console	Não	Sim
Usar a AWS Console Mobile Application	Não	Sim
Desativar o suporte ao console multissessão	Não	Sim. Se você entrar novamente usando um Builder ID, o suporte a várias sessões será ativado automaticamente.

Compare o gerenciamento de acesso

Quando você usa nossa nova AWS experiência, AWS cria padrões pré-configurados para ajudar você a começar a criar. Seus AWS recursos são organizados em projetos. Um projeto contém uma Conta da AWS, chamada de conta de projeto, e configurações para compartilhamento com outros colaboradores. Se você usa o plano pago, seu projeto também pode ter um custo mensal definido antes de impostos, chamado limite de gastos. Todos os projetos que você possui compõem sua organização, que você controla por meio de sua conta de gerenciamento nas AWS Configurações.

Essa organização é igual a uma AWS organização; no entanto, AWS gerencia aspectos dessa organização em seu nome.

AWS gerencia os seguintes elementos da sua AWS organização:

- Políticas de gerenciamento da organização. Quando você usa nossa nova AWS experiência, AWS gerencia as políticas de gerenciamento da organização, incluindo as políticas de controle de recursos (RCPs) e as políticas de controle de serviços (SCPs). Se você quiser criar o seu próprio, use Inscrever-se em AWS (avançado).
- Funções de acesso humano. Uma função de acesso humano é qualquer função que conceda permissões específicas a uma pessoa. AWS fornece a você e aos membros da sua equipe acesso de administrador aos seus projetos. Como proprietário do projeto, você pode adicionar e remover membros da equipe. Para obter mais informações, consulte [Convide membros da equipe para colaborar em AWS Configurações](#). Você não cria um usuário root. Seu ID do AWS Builder possui suas contas de projeto em vez de um endereço de e-mail do usuário root, e isso não muda quando você ativa recursos avançados. Você pode criar funções do IAM e usuários do IAM, se necessário, mas eles só podem ser usados para acesso programático, não para acesso ao console.

Cada projeto tem uma implementação de segurança gerenciada que facilita a criação com confiança. Por padrão, qualquer aplicativo ou código em seu projeto tem acesso a todos os AWS recursos desse mesmo projeto. Você não precisa realizar configurações adicionais de acesso.

AWS recursos em projetos diferentes não podem acessar uns aos outros, a menos que você ative o acesso entre projetos para determinados recursos. Por exemplo, você pode criar uma função Lambda em um projeto e depois invocá-la usando uma API em um projeto diferente. Isso é descrito como uma integração entre contas. Para obter mais informações, consulte [Integrações do Cross-accountLambda](#). Desde que ambos os projetos sejam de propriedade da mesma conta de gerenciamento, isso é suportado.

Por padrão, seu projeto não fornece acesso externo a nenhum recurso. Você deve configurar AWS os recursos para permitir o acesso público. Você pode fazer o seguinte:

- Crie um bucket público do S3 para hospedar um site ou arquivos estáticos simples. Para obter mais informações, consulte [Conceitos básicos do Amazon S3](#).
- Crie uma API do API Gateway para atuar como a porta de entrada do seu aplicativo. Para obter mais informações, consulte [Criar uma API HTTP](#).

- Crie uma instância do EC2 com um endereço IP público para permitir a comunicação entre suas instâncias e a Internet. Para obter mais informações, consulte [Iniciar sua primeira instância do EC2](#).
- Crie uma CloudFront distribuição para entregar seu conteúdo web estático e dinâmico, como arquivos de imagem, .html, .css, .js e arquivos de imagem, para seus usuários. Para obter mais informações, consulte [Introdução ao CloudFront](#).
- Crie uma URL de função Lambda para fornecer um endpoint HTTP simples, direto e acessível ao público para uma função Lambda. Certifique-se de que sua função Lambda tenha as permissões corretas. Para obter mais informações, consulte [Criação de uma URL de função](#) e [Modelo de segurança e autenticação para URLs de funções Lambda](#).
- Use uma combinação desses ou de outros AWS mecanismos.

Além disso, ao ativar recursos avançados, você tem acesso a ainda mais mecanismos para fornecer acesso externo aos seus recursos.

Gerencie seu Contas da AWS

Você gerencia seu Contas da AWS com base no tipo de AWS que está usando. A tabela a seguir mostra onde encontrar a documentação para cada tarefa de gerenciamento.

Tarefa	Inscreva-se para AWS (novo)	Inscreva-se para AWS (avançado)
Inscrever-se	Inscreva-se para AWS (novo)	Inscreva-se para AWS (avançado)
Criar uma conta da	Crie um projeto em AWS Configurações	Inscreva-se para AWS (avançado)
Encerrar uma conta	Fechar um projeto em AWS Configurações	Fechar um Conta da AWS
Atualize sua senha	Atualize sua senha em AWS Configurações	Atualizar senha do usuário-raiz

Tarefa	Inscreva-se para AWS (novo)	Inscreva-se para AWS (avanzado)
Registre dispositivos de MFA	Gerencie a autenticação multifatorial (MFA) no AWS Configurações	Etapa 3: (Recomendado) Configurar o AWS Servidor MCP
Alterar seu e-mail	Altere seu endereço de e-mail em AWS Configurações	Atualize o endereço de e-mail do usuário-raiz
Mude seu nome	Gerencie seu nome ou apelido em AWS Configurações	Atualize seu Conta da AWS name
Atualizar informações de contato	Edite suas informações de contato em AWS Configurações	Atualize o contato principal do seu Conta da AWS
Atualizar contatos alternativos	Não aplicável	Atualize os contatos alternativos para seu Conta da AWS
Gerenciar o faturamento	Gerencie sua forma de pagamento em AWS Configurações	Atualize o faturamento do seu Conta da AWS
Gerenciar informações fiscais	Gerencie o registro fiscal em AWS Configurações	Gerencie seus pagamentos
Ativar ou desativar Regiões da AWS	Não aplicável. Você não pode modificar seu Região da AWS.	Ativar ou desativar Regiões da AWS na sua conta
Exibir identificadores de conta	Não aplicável	Visualizar Conta da AWS identificadores

Tarefa	Inscreva-se para AWS (novo)	Inscreva-se para AWS (avanzado)
Criar um alias de conta	Não aplicável	Crie um Conta da AWS alias
Atualize sua conta	Atualize sua conta em AWS Configurações	Planos de nível gratuito
Criar um limite de gastos	Crie um limite de gastos em AWS Configurações	Não aplicável
Atualizar um limite de gastos	Atualizar um limite de gastos em AWS Configurações	Não aplicável
Remover um limite de gastos	Remova um limite de gastos em AWS Configurações	Não aplicável
Convide membros da equipe	Convide membros da equipe para colaborar em AWS Configurações	Identidades do IAM
Alternar entre projetos	Alternar entre projetos	Multi-session apoio
Connect uma ferramenta de codificação de IA	Conecte uma ferramenta de codificação de IA	Não aplicável
Excluir todas as sessões	Excluir todas as sessões em AWS Configurações	Não aplicável

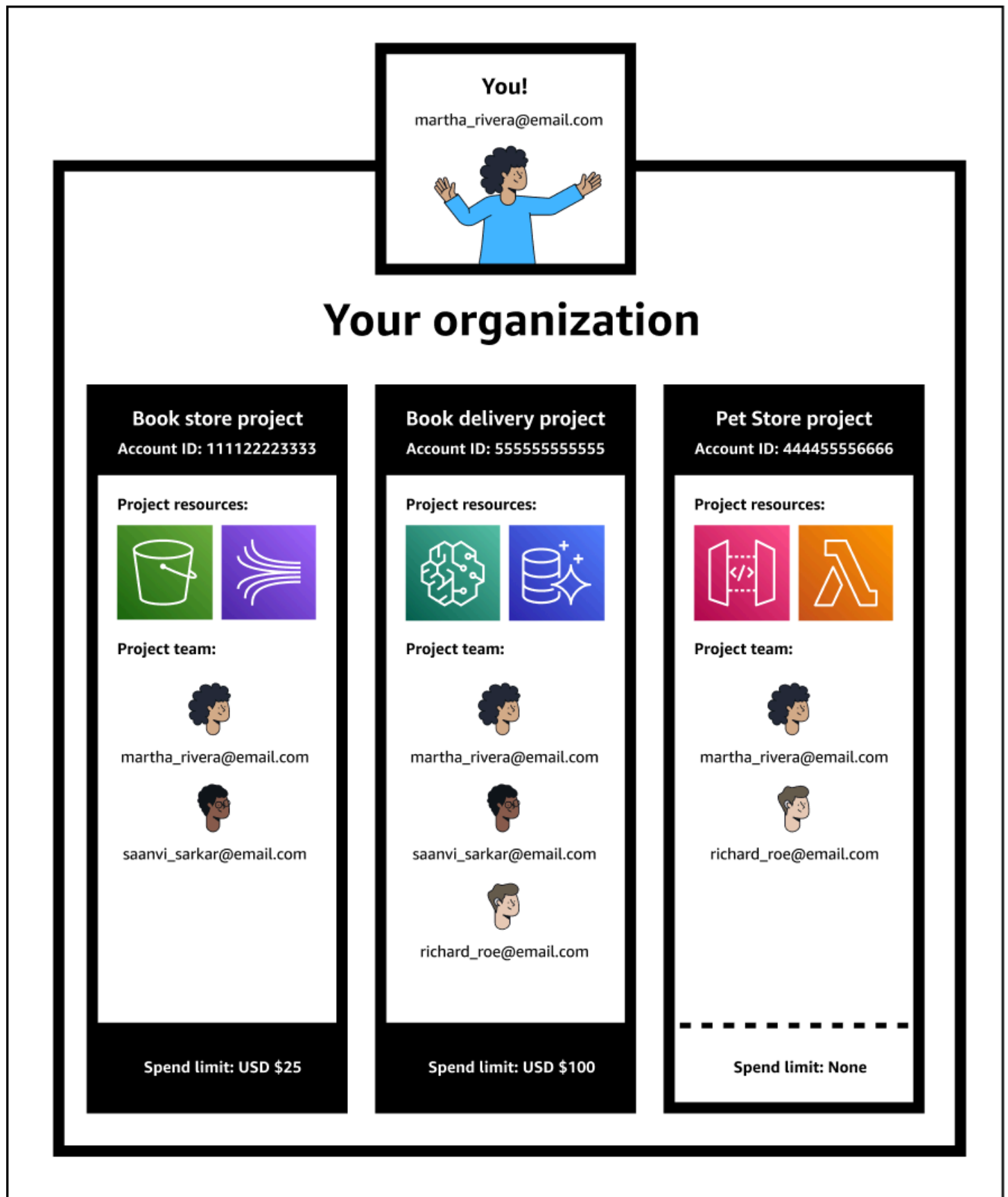
Tarefa	Inscreva-se para AWS (novo)	Inscreva-se para AWS (avançado)
Optar por não usar dados de IA	Opte por não usar seu conteúdo para melhorar o serviço em AWS Configurações	Políticas de recusa de serviços de IA
Solicitar seus dados do	Solicite seu AWS Dados de ID do Builder	Solicite seus dados
Exclua seu AWS perfil	Feche sua conta em AWS Configurações	Fechar um Conta da AWS
Gerenciar contas na Índia	Gerencie contas na Índia em AWS Configurações	Gerenciar contas na Índia
Criação de um usuário administrador	Não aplicável	Inscreva-se para AWS (avançado)
Planeje sua estrutura de governança de contas	Não aplicável	Planeje seu Conta da AWS estrutura de governança

Inscriva-se para AWS (novo)

Warning

No momento, estamos lançando nossa nova experiência para um número limitado de clientes. Talvez você ainda não consiga acessar essa experiência.

Ao usar o Sign up for AWS (new), você cria um AWS ambiente pré-configurado que permite usar um login que você já possui, como o Google, ou GitHub para acessar seus AWS recursos. Seus recursos são organizados em projetos. Um projeto contém configurações Conta da AWS e para compartilhamento com outros colaboradores. Se você usa o plano pago, seu projeto também pode ter um custo mensal definido antes de impostos, chamado limite de gastos. Todos os projetos que você possui compõem sua organização. Você gerencia sua organização, acessa seus projetos e adiciona membros da equipe nas AWS Configurações.



Quando você se inscreve para AWS usar o Sign up for AWS (new), AWS também cria uma ID do builder AWS conta, que é um perfil pessoal que representa você como indivíduo. Você só pode ter um ID do builder AWS para cada endereço de e-mail. Se você criou um, ID do builder AWS mas não criou um Conta da AWS, talvez já tenha algumas configurações feitas para você e precisará modificá-las posteriormente.

Para obter mais informações sobre Inscrever-se em AWS (novo), consulte a seguinte documentação:

- [Compare as opções de inscrição](#)
- [Compatível Serviços da AWS para Inscreva-se em AWS \(novo\)](#)

Inscreva-se usando Inscrever-se em AWS (novo)

Quando você se inscreve AWS, podemos solicitar informações de pagamento. Nosso processo de verificação retém USD \$1 (ou equivalente) por 3 a 5 dias para verificar sua conta e evitar fraudes. Você não incorrerá em cobranças até fazer o upgrade para um plano pago. Você pode gerenciar sua forma de pagamento ou fechar suas contas a qualquer momento por meio das AWS Configurações. Além disso, ao se inscrever AWS, você pode não se qualificar para o nível gratuito. Nesse caso, você precisará fornecer suas informações de pagamento e será colocado no plano pago. Quando você está no plano pago, você pode definir limites de gastos para operar dentro de um orçamento previsível e controlado.

Inscreva-se para receber AWS (novos) suportes usando o Google GitHub, a Apple ou a Amazon para sua conta. Se você já estiver conectado a uma conta do Google no seu navegador, essa conta será usada quando você se inscrever AWS.

Para se inscrever em AWS usando Inscrever-se para AWS (novo)

1. Abra a página [Cadastrar-se na AWS](#).
2. Digite seu e-mail ou escolha um login, como Google GitHub, Apple ou Amazon.
3. Se você usar um login que já possui, será direcionado para o login do seu provedor. Depois de fazer login, você será redirecionado para se AWS inscrever.
4. Digite seu nome e escolha Continuar.

Esse nome é compartilhado com os membros da equipe quando você dá acesso aos seus projetos.

5. Verifique o e-mail associado ao seu login inserindo um código de verificação. Depois de verificar seu e-mail, escolha Continuar.

Esse e-mail é compartilhado com os membros da equipe quando você dá acesso aos seus projetos.

6. Insira uma senha forte para sua conta e escolha Continuar.

AWS exige que sua senha atenda às seguintes condições:

- Ter no mínimo 8 caracteres e no máximo 128 caracteres de extensão.
- Incluir no mínimo três dos seguintes tipos de caracteres: maiúsculas, minúsculas, números e os símbolos ! @ # \$ % ^ & * () < > [] { } | _ + =.
- Não deve ser idêntico ao seu Conta da AWS nome ou endereço de e-mail.

7. Insira seus dados de contato e escolha Continuar.

8. AWS provisionará seu primeiro projeto em um dos três Regiões da AWS com um novo nome. Para obter mais informações, consulte [Regiões da AWS para seus projetos](#). Você pode alterar o nome a qualquer momento.

Agora você pode acessar Console de gerenciamento da AWS o. Para acessar AWS as Configurações, escolha Gerenciar projetos no Console de gerenciamento da AWS. Em AWS Configurações, você pode convidar membros da equipe, criar novos projetos e modificar seu faturamento e outras configurações.

Próximas etapas

Depois de se inscrever AWS, você pode conectar uma ferramenta de codificação de IA, adicionar membros da equipe para colaborar e, se tiver um plano pago, criar um limite de gastos.

- [Conecte uma ferramenta de codificação de IA](#)
- [Convide membros da equipe para colaborar em AWS Configurações](#)
- [Crie um limite de gastos em AWS Configurações](#)

Use AWS Configurações

Warning

No momento, estamos lançando nossa nova experiência para um número limitado de clientes. Talvez você ainda não consiga acessar essa experiência.

[AWS As configurações](#) são onde você gerencia e acessa seus projetos. AWS As configurações estão disponíveis quando você se inscreve usando o Sign up for AWS (novo). Você pode usar AWS as Configurações para fazer o seguinte:

- Crie e acesse projetos que você possui. Para obter mais informações, consulte [Crie um projeto em AWS Configurações](#).
- Acesse projetos que foram compartilhados com você.
- Convide membros da equipe para colaborar em seus projetos. Para obter mais informações, consulte [Convide membros da equipe para colaborar em AWS Configurações](#).
- Alterne entre projetos. Para obter mais informações, consulte [Alternar entre projetos](#).
- Gerencie sua forma de pagamento. Para obter mais informações, consulte [Gerencie sua forma de pagamento em AWS Configurações](#).
- Faça o upgrade do nível gratuito para um plano pago. Para obter mais informações, consulte [Atualize sua conta em AWS Configurações](#).
- Gerencie os limites de gastos para seus projetos. Para obter mais informações, consulte [Crie um limite de gastos em AWS Configurações](#).
- Visualize suas informações de cobrança. Para obter mais informações, consulte [Visualize suas informações de cobrança em AWS Configurações](#).
- Gerencie as informações do seu perfil. Para obter mais informações, consulte [Gerencie seu nome ou apelido em AWS Configurações](#), [Altere seu endereço de e-mail em AWS Configurações](#) e [Edite suas informações de contato em AWS Configurações](#).
- Gerencie suas configurações de segurança e preferências de login. Para obter mais informações, consulte [Atualize sua senha em AWS Configurações](#) e [Gerencie a autenticação multifatorial \(MFA\) no AWS Configurações](#).

Ao gerenciar suas informações de perfil ou suas configurações de segurança, você será redirecionado para o ID do builder AWS hub. ID do builder AWS O seu é criado quando você usa o Sign up for AWS (novo). Para obter mais informações, consulte [O que é ID do builder AWS?](#).

Conecte uma ferramenta de codificação de IA

Warning

No momento, estamos lançando nossa nova experiência para um número limitado de clientes. Talvez você ainda não consiga acessar essa experiência.

Você pode fornecer à sua ferramenta de codificação de IA acesso ao seu projeto e instalar o Agent Toolkit, que agrupa a configuração do servidor AWS MCP e um conjunto selecionado de habilidades do agente. Isso permite que sua ferramenta de codificação de IA crie e gerencie AWS recursos em seu nome.

Considerações para conectar sua ferramenta de codificação ao seu projeto

- Você pode conectar ferramentas de codificação de IA a um projeto que você possui ou a um projeto que foi compartilhado com você.
- Quando uma ferramenta de codificação de IA ou um agente local cria AWS recursos, você ainda é responsável por eles. Isso inclui a segurança adequada de seus recursos, conforme definido pelo modelo de responsabilidade [compartilhada](#), e quaisquer cobranças que possam ocorrer com esses recursos, sejam elas contabilizadas no Plano Gratuito ou cobradas no Plano Pago.
- Você é responsável por todas as ações que sua ferramenta de codificação de IA realiza em seu nome em seus projetos.
- Para visualizar um recurso que seu agente criou, acesse o console de serviço desse serviço.
- As credenciais que você gera são para uso pelo AWS CLI, AWS Tools for PowerShell e AWS SDKs. Ferramentas externas podem não ser suportadas. O acesso aos seus recursos é válido por 12 horas. Use o comando a seguir para renovar suas credenciais:

```
aws login --profile profile-name
```

profile-name Substitua pelo nome do perfil que você escolheu durante a configuração inicial. O comando abrirá automaticamente seu navegador padrão. Você precisará escolher o nome do seu

projeto para concluir o processo de login. AWS pode renovar suas credenciais por 90 dias. Depois de 90 dias, você precisará conceder acesso novamente em uma janela do navegador.

Conecte sua ferramenta de codificação de IA ao seu projeto

Cada projeto tem seu próprio conjunto de credenciais que as ferramentas de codificação de IA podem usar para criar e gerenciar AWS recursos em seu nome.

Console de gerenciamento da AWS

Para conectar sua ferramenta de codificação de IA ao seu projeto usando o AWS console

1. Abra AWS as configurações em <https://settings.aws.com>.
2. No painel de navegação principal, escolha o projeto que você deseja acessar.
3. Na barra de navegação no canto superior direito, escolha Criar e gerenciar infraestrutura em nuvem.
4. Escolha Usar suas AWS credenciais com ferramentas de codificação de IA.
5. Escolha Copiar prompt do agente e insira-o em seu agente de codificação.

Isso cria um prompt que compartilha um arquivo de direção com seu agente de codificação de IA. O arquivo de direção acessa um script AWS que configura a conexão entre suas credenciais de projeto e seu agente de codificação de IA.

Você inserirá um nome de perfil para o seu projeto. Esse nome de perfil é como sua ferramenta de codificação de IA acessa seus recursos.

Use your terminal

Execute o comando a seguir para fazer o download e siga as instruções de configuração:

```
curl -fsSL https://github.com/aws/agent-toolkit-for-aws/blob/main/setup-instructions/setup.md
```

Ao usar nossa nova AWS experiência, seu agente instalará o servidor AWS MCP e você terá acesso às habilidades do agente que podem ser usadas em seus projetos. Você também receberá um arquivo de regras com orientações ajustadas para essa experiência. O arquivo de regras também

permitirá que você defina o nível de ajuda que você deseja que o agente forneça. A seguir estão os níveis de ajuda suportados:

- Baixo: enquanto você estiver construindo, a habilidade só sinalizará riscos de segurança. Isso não sugerirá nenhuma melhoria ou alternativa à sua arquitetura.
- Médio: enquanto você está construindo, a habilidade pode fazer algumas perguntas esclarecedoras se detectar possíveis problemas. Isso não sugerirá nenhuma melhoria ou alternativa à sua arquitetura.
- Alto: Enquanto você estiver construindo, a habilidade fornecerá um alto nível de suporte. Isso sugerirá melhorias ou alternativas à sua arquitetura.

Trabalhe com vários projetos

Cada projeto tem seu próprio conjunto de credenciais que as ferramentas de codificação de IA podem usar para criar e gerenciar AWS recursos em seu nome. Você usa perfis para acessar cada projeto. Um perfil é uma configuração e um arquivo de credenciais mantido pelo AWS CLI, e você atribui a cada perfil um nome exclusivo.

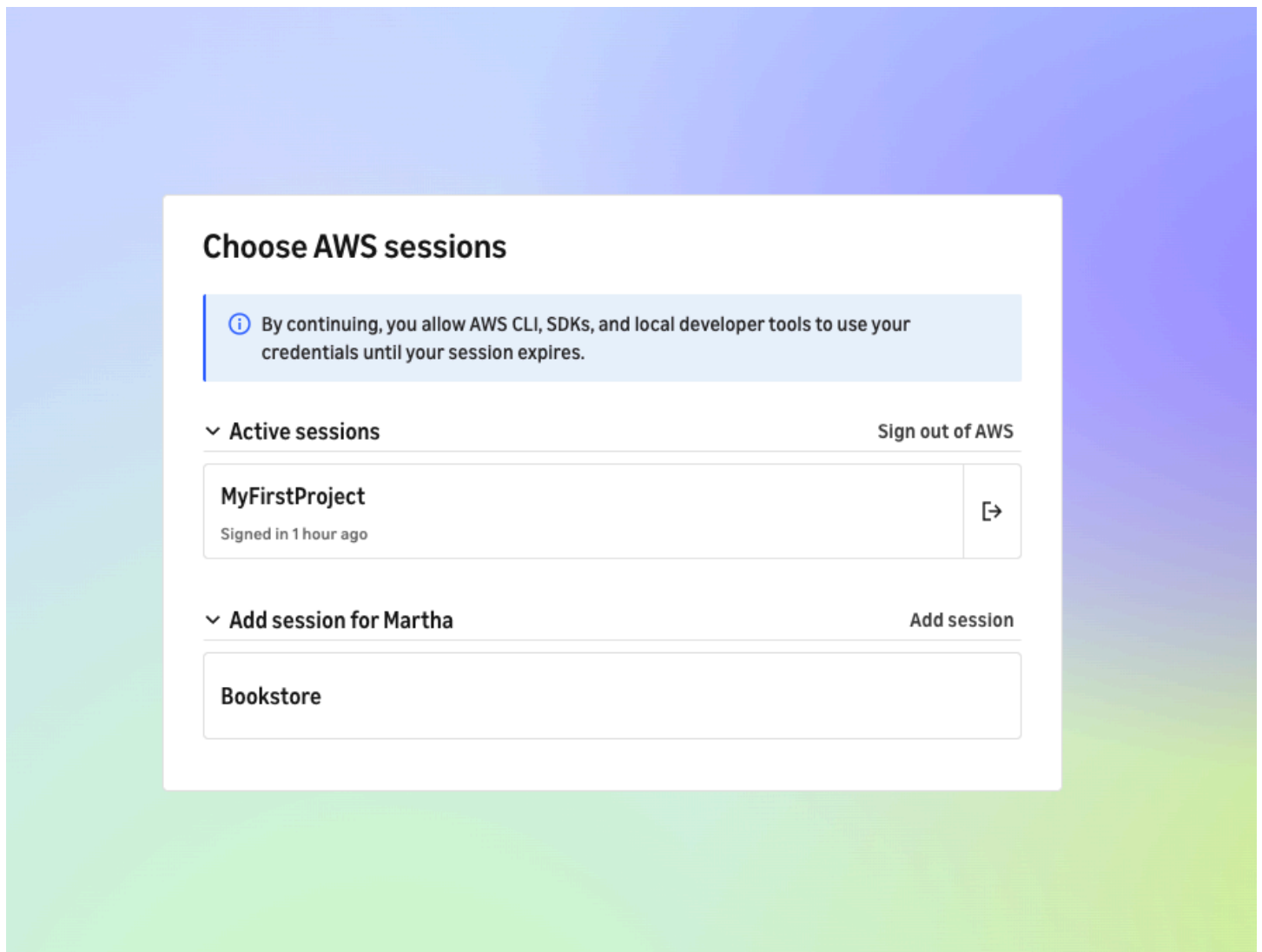
Por exemplo, se seu primeiro projeto foi `MyFirstProject` e você escolheu o nome do perfil `MyFirstProjectProfile` durante a configuração, você pode acessar esse projeto fazendo login no AWS CLI com o seguinte comando:

```
aws login --profile MyFirstProjectProfile
```

Se você criar outro projeto chamado `Bookstore`, poderá acessá-lo usando o script de configuração e criando o perfil `BookstoreProfile`. Em seguida, você pode fazer login no AWS CLI com o seguinte comando:

```
aws login --profile BookstoreProfile
```

No entanto, ao executar qualquer um desses comandos, você precisará escolher uma sessão para suas AWS credenciais na página [Escolher AWS sessões](#).



Esta página mostra as sessões ativas e as sessões que você pode adicionar. Uma sessão representa seu estado autenticado com suas AWS credenciais e fornece as mesmas credenciais que seu agente de codificação de IA usa para criar e gerenciar recursos.

Neste exemplo, você já fez login MyFirstProject e não fez login. Bookstore Na página Escolher AWS sessões, você pode fazer o seguinte:

- Para continuar usando AWS forMyFirstProject, escolhaMyFirstProject.
- Para acessarBookstore, escolhaBookstore.
- Para remover qualquer uma das sessões atuais, escolha o ícone de saída.
- Para acessar e Conta da AWS usar um usuário do IAM, como uma conta que você criou com[Inscreva-se para AWS \(avançado\)](#), escolha Adicionar sessão.

As credenciais que você escolher serão as mesmas que seu agente de codificação de IA usa para criar e gerenciar recursos. Por exemplo, você pode fazer login no AWS CLI com o seguinte comando:

```
aws login --profile MyFirstProjectProfile
```

Se você escolher a Bookstore sessão, sua ferramenta de codificação de IA criará AWS recursos no Bookstore projeto.

Sempre escolha a sessão que corresponda ao projeto associado ao seu perfil.

AWS ações para proprietários de projetos

Warning

No momento, estamos lançando nossa nova experiência para um número limitado de clientes. Talvez você ainda não consiga acessar essa experiência.

Quando você é proprietário do seu projeto, você tem controle administrativo sobre ele. Isso inclui tarefas que você pode concluir em [Use AWS Configurações](#). Você também tem a capacidade de realizar ações somente root. Essas ações não podem ser concluídas pelos membros da sua equipe.

As ações atuais somente de root que você pode realizar são as seguintes:

- Edite ou exclua uma política de bucket do S3 que nega todos os principais. Você pode fazer isso para desbloquear um bucket do S3 com uma política de bucket mal configurada.
- Edite ou exclua uma política baseada em recursos do SQS que nega todos os diretores. Você pode fazer isso para desbloquear uma fila SQS com uma política baseada em recursos mal configurada.

Para realizar uma ação somente root

1. Faça login em seu projeto e abra o console do IAM em <https://console.aws.amazon.com/iam/>.
2. No painel de navegação do console, escolha Gerenciamento de acesso raiz.
3. Para ação privilegiada, escolha a ação privilegiada que você deseja realizar na conta do membro.

- Selecione Excluir política de bucket do Amazon S3 para remover uma política de bucket mal configurada que impeça que todas as entidades principais acessem o bucket do Amazon S3.
 - a. Insira o URI do S3 ou escolha `Browse S3` para selecionar um nome dos buckets em seu projeto.
 - b. Escolha Excluir política de bucket.
 - c. Use o console do Amazon S3 para corrigir a política de bucket após excluir a política mal configurada. Para obter mais informações, consulte [Adição de uma política de bucket com o console do Amazon S3](#) no Guia do usuário do Amazon S3.
- Selecione Excluir política do Amazon SQS para excluir uma política baseada em recursos que impede que todos os diretores acessem uma fila do Amazon SQS.
 - a. Insira o nome da fila em Nome da fila `SQS`.
 - b. Escolha Excluir política `SQS`.
 - c. Use o console do Amazon SQS para corrigir a política de fila após excluir a política mal configurada. Para obter mais informações, consulte [Configuração de uma política de acesso no Amazon SQS](#), no Guia do desenvolvedor do Amazon SQS.

Atualize sua senha em AWS Configurações

Warning

No momento, estamos lançando nossa nova experiência para um número limitado de clientes. Talvez você ainda não consiga acessar essa experiência.

Você pode atualizar sua senha em AWS Configurações.

Para atualizar sua senha no AWS Configurações

1. Abra AWS as configurações em <https://settings.aws.com>.
2. No painel de navegação principal, escolha `Gerenciar segurança e login`.

Você será redirecionado para o seu perfil AWS Builder ID.

3. Em `Autorização`, escolha `Atualizar senha`.

4. Em Current password (Senha atual), insira a sua senha atual.
5. Em Nova senha, insira uma nova senha.

AWS exige que sua senha atenda às seguintes condições:

- Ter no mínimo 8 caracteres e no máximo 128 caracteres de extensão.
 - Incluir no mínimo três dos seguintes tipos de caracteres: maiúsculas, minúsculas, números e os símbolos ! @ # \$ % ^ & * () < > [] { } | _ + = .
6. Em Confirmar nova senha, insira sua nova senha.
 7. Selecione Atualizar.

Gerencie a autenticação multifatorial (MFA) no AWS Configurações

Warning

No momento, estamos lançando nossa nova experiência para um número limitado de clientes. Talvez você ainda não consiga acessar essa experiência.

Multi-factor a autenticação (MFA) é um mecanismo simples e eficaz para aprimorar sua segurança. O primeiro fator, sua senha, é um segredo que você memoriza, também conhecido como fator de conhecimento. Outros fatores podem ser fatores de posse (algo que você tem, como uma chave de segurança) ou fatores de inerência (algo que você é, como um escaneamento biométrico). É altamente recomendável que você configure o MFA para adicionar uma camada adicional à sua conta.

Você pode registrar um autenticador incorporado e também uma chave de segurança que você mantém em um local fisicamente seguro. Se você não conseguir usar o autenticador integrado, poderá usar sua chave de segurança registrada. Para aplicativos autenticadores, você também pode ativar o atributo de backup ou sincronização na nuvem nesses aplicativos. Isso ajuda a evitar a perda de acesso ao seu perfil se você perder ou quebrar seu dispositivo de MFA.

Principais pontos

Lembre-se dos seguintes pontos-chave ao registrar e gerenciar dispositivos de MFA:

- Recomendamos que você registre vários dispositivos de MFA. Se você perder o acesso a todos os dispositivos de MFA registrados, não conseguirá recuperar sua conta.

- Recomendamos que você revise periodicamente seus dispositivos de MFA registrados para garantir que estejam atualizados e funcionais. Além disso, você deve armazenar esses dispositivos em um local fisicamente seguro quando não estiverem em uso.
- Se você criou sua conta usando Continuar com o Google, pode ativar a autenticação multifator por meio de sua conta do Google. Para obter detalhes, consulte [Turn on 2-Step Verification](#).
- Se você criou sua conta usando Continuar com a Apple, a autenticação multifator provavelmente já está ativada em sua conta Apple. Caso contrário, para obter detalhes sobre como ativá-la, consulte a [Two-factor autenticação da Conta Apple](#).
- Se você criou sua conta usando Continuar com GitHub, você pode ativar a autenticação multifator por meio de sua GitHub conta. Para obter detalhes, consulte [Configurando \(GitHub\) a autenticação de dois fatores](#).
- Se você criou sua conta usando Continuar com a Amazon, você pode habilitar a autenticação multifator por meio de sua conta da Amazon. Para obter detalhes, consulte [O que é Two-Step verificação?](#).

Tipos de MFA disponíveis para nosso novo AWS experiência

Nossa nova AWS experiência oferece suporte aos seguintes tipos de dispositivos de autenticação multifator (MFA).

Autenticadores FIDO2

[O FIDO2](#) é um padrão que inclui CTAP2 [WebAuthn](#) e é baseado na criptografia de chave pública. As credenciais FIDO são resistentes ao phishing porque são exclusivas do site em que as credenciais foram criadas, como a AWS.

AWS suporta os dois formatos mais comuns dos autenticadores FIDO: autenticadores integrados e chaves de segurança. Veja abaixo mais informações sobre os tipos mais comuns de autenticadores FIDO.

Built-in autenticadores

Alguns dispositivos têm autenticadores integrados, como o TouchID MacBook ou uma câmera Windows Hello-compatible. Se o seu dispositivo for compatível com os protocolos FIDO, inclusive WebAuthn, você pode usar sua impressão digital ou rosto como segundo fator. Para obter mais informações, consulte [Autenticação FIDO](#).

Chaves de segurança

Você pode comprar um USB FIDO2-compatible externo, BLE ou chave NFC-connected de segurança. Quando você for solicitado a inserir um dispositivo de MFA, toque no sensor da tecla. YubiKey Para a Feitian, faça dispositivos compatíveis. Para obter uma lista de todas as chaves de segurança compatíveis, consulte [Produtos certificados pela FIDO](#).

Gerenciadores de senhas, fornecedores de chaves de acesso e outros autenticadores FIDO

Vários provedores terceirizados oferecem suporte à autenticação FIDO em aplicativos móveis, como atributos em gerenciadores de senhas, cartões inteligentes com modo FIDO, entre outros formatos. Esses FIDO-compatible dispositivos podem funcionar com o IAM Identity Center, mas recomendamos que você mesmo teste um autenticador FIDO antes de ativar essa opção para MFA.

Note

Alguns autenticadores FIDO podem criar credenciais FIDO detectáveis, conhecidas como chaves de acesso. As chaves de acesso podem estar vinculadas ao dispositivo que as criou, ou podem ser sincronizadas e armazenadas em uma nuvem. Por exemplo, você pode registrar uma chave de acesso usando o Apple Touch ID em um Macbook compatível e, em seguida, fazer login em um site a partir de um laptop Windows usando o Google Chrome com sua chave de acesso no iCloud, seguindo as instruções na tela ao fazer login. Para obter mais informações sobre quais dispositivos são compatíveis com chaves de acesso sincronizáveis e a interoperabilidade atual de chaves de acesso entre sistemas operacionais e navegadores, consulte [Device Support](#) em passkeys.dev, um recurso mantido pela FIDO Alliance And World Wide Web Consortium (W3C).

Aplicativos autenticadores

Os aplicativos autenticadores são autenticadores terceirizados baseados em senha de uso único (OTP). Você pode usar um aplicativo autenticador instalado em seu dispositivo móvel ou tablet como um dispositivo de MFA autorizado. O aplicativo autenticador de terceiros deve estar em conformidade com RFC 6238, que é um algoritmo de senha de uso único com marcação temporal (TOTP) padrão capaz de gerar códigos de autenticação de seis dígitos.

Quando a MFA for solicitada, você deve inserir um código válido do seu aplicativo autenticador na caixa de entrada apresentada. Cada dispositivo MFA atribuído a um usuário deve ser exclusivo. Dois aplicativos autenticadores podem ser registrados para qualquer usuário.

Você pode escolher entre os seguintes aplicativos autenticadores de terceiros conhecidos. No entanto, qualquer TOTP-compliant aplicativo funciona com o AWS Builder ID MFA.

Sistema operacional	Aplicativo autenticador testado
Android	1Password , Authy , Duo Mobile , Microsoft Authenticator , Google Authenticator
iOS	1Password , Authy , Duo Mobile , Microsoft Authenticator , Google Authenticator

Registrar seu dispositivo de MFA do

Note

Depois de se inscrever no MFA, sair e entrar no mesmo dispositivo, talvez você não seja solicitado a inserir a MFA em dispositivos confiáveis.

Como registrar seu dispositivo de MFA usando um aplicativo autenticador

1. Abra AWS as Configurações em <https://settings.aws.com>.
2. No painel de navegação principal, escolha Gerenciar segurança e login.

Você será redirecionado para o seu perfil AWS Builder ID.

3. Na página Segurança, selecione Registrar dispositivo.
4. Na página Registrar dispositivo de MFA, selecione Aplicativo autenticador.
5. AWS O Builder ID opera e exibe informações de configuração, incluindo um gráfico de código QR. O gráfico é uma representação da “chave de configuração secreta” que está disponível para entrada manual em aplicativos autenticadores que não suportam códigos QR.
6. Abra seu aplicativo autenticador. Para obter uma lista de aplicativos, consulte [Aplicativos autenticadores](#).

Se o aplicativo autenticador oferecer suporte a vários dispositivos ou contas de MFA, selecione a opção para criar uma nova conta ou dispositivo de MFA.

7. Determine se o aplicativo de MFA é compatível com códigos QR e, em seguida, execute uma das seguintes ações na página Configurar seu aplicativo autenticador:
 1. Escolha Mostrar código QR e, em seguida, use o aplicativo para digitalizar o código QR. Por exemplo, você pode escolher o ícone de câmera ou escolher uma opção semelhante a Digitalizar código. Em seguida, use a câmera do dispositivo para digitalizar o código.
 2. Escolha Mostrar chave secreta e, em seguida, insira essa chave secreta em seu aplicativo de MFA.

Quando você concluir, seu aplicativo autenticador gerará e exibirá uma senha de uso único.

8. Na caixa Código do autenticador, insira a senha de uso único que atualmente é exibida no aplicativo autenticador. Escolha Assign MFA.

 Important

Envie sua solicitação imediatamente após gerar o código. Se você gerar o código e esperar muito tempo para enviar a solicitação, o dispositivo de MFA será associado com sucesso à sua ID do AWS construtor, mas o dispositivo de MFA ficará fora de sincronia. Isso ocorre porque as senhas únicas baseadas em tempo (time-based one-time passwords, TOTP) expiram após um curto período. Caso isso ocorra, você pode resincronizar o dispositivo. Para obter mais informações, consulte *I get the message 'An unexpected error has occurred' when I try to register or sign in with an authenticator app*.

9. Para dar ao seu dispositivo um nome amigável no AWS Builder ID, escolha Renomear. Esse nome ajuda você a distinguir esse dispositivo de outros que você registra.

O dispositivo de MFA agora está pronto para ser usado com AWS as Configurações, seus projetos e o AWS Builder ID.

Registrar uma chave de segurança como seu dispositivo de MFA do

Como registrar seu dispositivo de MFA usando uma chave de segurança

1. Abra AWS as Configurações em <https://settings.aws.com>.
2. No painel de navegação principal, escolha Gerenciar segurança e login.

Você será redirecionado para o seu perfil AWS Builder ID.

3. Na página Segurança, selecione Registrar dispositivo.
4. Na página Registrar dispositivo de MFA, selecione Chave de segurança.
5. Verifique se sua chave de segurança está habilitada. Se você usar uma chave de segurança física separada, conecte-a ao seu computador.
6. Siga as instruções na tela. Sua experiência varia de acordo com seu sistema operacional e navegador.
7. Para dar ao seu dispositivo um nome amigável no AWS Builder ID, escolha Renomear. Esse nome ajuda você a distinguir esse dispositivo de outros que você registra.

O dispositivo de MFA agora está pronto para ser usado com AWS as Configurações, seus projetos e o AWS Builder ID.

Renomear seu dispositivo de MFA do

Como renomear um dispositivo de MFA

1. Abra AWS as Configurações em <https://settings.aws.com>.
2. No painel de navegação principal, escolha Gerenciar segurança e login.

Você será redirecionado para o seu perfil AWS Builder ID.

3. Selecione Segurança. Ao chegar à página, você vê que a opção Renomear está esmaecida.
4. Selecione o dispositivo de MFA que você deseja alterar. Isso permite que você selecione Renomear. Em seguida, é exibida uma caixa de diálogo.
5. No prompt aberto, insira o novo nome no nome do dispositivo de MFA e selecione Renomear. O dispositivo renomeado aparece em dispositivos de Multi-factor autenticação (MFA).

Exclua seu dispositivo de MFA

Recomendamos que você mantenha dois ou mais dispositivos de MFA ativos. Para desativar a autenticação multifator, remova todos os dispositivos de MFA registrados do seu perfil.

Como excluir um dispositivo de MFA

1. Abra AWS as Configurações em <https://settings.aws.com>.

2. No painel de navegação principal, escolha Gerenciar segurança e login.

Você será redirecionado para o seu perfil AWS Builder ID.

3. Na página Segurança, selecione o dispositivo de MFA que você deseja alterar e escolha Excluir.
4. Na caixa de diálogo modal Excluir dispositivo de MFA?, siga as instruções para excluir seu dispositivo.
5. Escolha Excluir.

O dispositivo excluído não aparece mais em dispositivos de Multi-factor autenticação (MFA).

Excluir todas as sessões em AWS Configurações

Warning

No momento, estamos lançando nossa nova experiência para um número limitado de clientes. Talvez você ainda não consiga acessar essa experiência.

Você pode excluir todas as sessões em todos os dispositivos nas AWS Configurações. Se houver um dispositivo que você não reconhece, altere sua senha e exclua todas as sessões.

Para excluir todas as sessões

1. Abra AWS as configurações em <https://settings.aws.com>.
2. No painel de navegação principal, escolha Gerenciar segurança e login.

Você será redirecionado para o seu perfil AWS Builder ID.

3. Em Dispositivos conectados, escolha Excluir todas as sessões.
4. Confirme sua escolha e escolha Excluir todas as sessões.

Você será desconectado das AWS Configurações.

Gerencie seu nome ou apelido em AWS Configurações

Warning

No momento, estamos lançando nossa nova experiência para um número limitado de clientes. Talvez você ainda não consiga acessar essa experiência.

Você pode alterar seu nome a qualquer momento. Todos os membros da equipe podem ver seu nome e, se você fez o upgrade para o plano pago, esse é o nome que aparece nas suas informações de cobrança. Se você se inscreveu AWS na Índia, seu nome deve corresponder exatamente ao nome que aparece no documento que você planeja usar para verificação do cliente.

Ao alterar seu nome, você altera o nome no seu AWS Builder ID. Isso afetará seu nome nas AWS Configurações, no AWS Builder ID e em quaisquer AWS recursos que você acesse diretamente por meio do AWS Builder ID.

Seu nome é a forma como você é mencionado em ferramentas e serviços enquanto interage com outras pessoas. Seu apelido indica como você quer ser conhecido AWS, amigos e outras pessoas com quem você colabora de perto.

Para alterar seu nome ou apelido

1. Abra AWS as configurações em <https://settings.aws.com>.
2. No painel de navegação principal, escolha Gerenciar perfil.
3. Para informações do perfil, escolha Gerenciar perfil.

Você será redirecionado para o seu perfil AWS Builder ID.

4. Para obter informações de perfil, escolha Editar.
5. (Opcional) Em Nome, insira um novo nome.
6. (Opcional) Em Apelido, insira um novo apelido.
7. Escolha Salvar alterações.

Altere seu endereço de e-mail em AWS Configurações

Warning

No momento, estamos lançando nossa nova experiência para um número limitado de clientes. Talvez você ainda não consiga acessar essa experiência.

Você pode alterar seu e-mail nas AWS Configurações. Quando você altera seu e-mail, seu e-mail anterior será separado do seu AWS perfil e do ID do AWS Builder. Você não poderá usar esse e-mail para acessar nenhum dos projetos nas AWS Configurações, mas poderá usar esse e-mail para se inscrever AWS novamente.

Seu endereço de e-mail é compartilhado com os membros da equipe quando você dá acesso aos seus projetos.

Para alterar seu e-mail

1. Abra AWS as Configurações em <https://settings.aws.com>.
2. No painel de navegação principal, escolha Gerenciar perfil.
3. Para informações do perfil, escolha Gerenciar perfil.

Você será redirecionado para o seu perfil AWS Builder ID.

4. Para informações de contato, escolha Editar.
5. Em Endereço de e-mail, insira um novo endereço de e-mail e escolha Verificar e-mail.
Enviaremos um código de verificação para seu novo endereço de e-mail. Isso será inserido na caixa pop-up Verificar e-mail.
6. Em Código de verificação, insira o código de verificação que enviamos para seu novo e-mail.
7. Escolha Verificar.

Edite suas informações de contato em AWS Configurações

Warning

No momento, estamos lançando nossa nova experiência para um número limitado de clientes. Talvez você ainda não consiga acessar essa experiência.

Você pode editar seu número de telefone ou endereço associado às AWS Configurações. Quando você modifica esses valores, eles podem afetar as obrigações fiscais.

Para editar suas informações de contato

1. Abra AWS as configurações em <https://settings.aws.com>.
2. No painel de navegação principal, escolha Gerenciar perfil.
3. Para informações de contato, escolha Editar.
4. Insira as novas informações de contato.
5. Escolha Salvar.

Opte por não usar seu conteúdo para melhorar o serviço em AWS Configurações

Warning

No momento, estamos lançando nossa nova experiência para um número limitado de clientes. Talvez você ainda não consiga acessar essa experiência.

AWS Os serviços de IA podem usar e armazenar o conteúdo do cliente para melhorar o serviço, como corrigir problemas operacionais, avaliar o desempenho do serviço, depurar ou treinar modelos. Para esse fim, podemos armazenar esse conteúdo Região da AWS fora do Região da AWS local em que você está usando o serviço. Você pode optar por não usar seu conteúdo para melhorar o serviço por meio das AWS Configurações. O efeito da exclusão é que AWS anexa uma política de exclusão de serviços de IA à sua organização. AWS Para obter mais informações sobre políticas de exclusão, consulte a documentação das políticas de exclusão de serviços de [IA](#).

Optar por não receber todos os serviços excluirá todos os seus projetos das melhorias de serviço usando seu conteúdo para serviços de IA suportados atuais e futuros, apoiados por políticas de exclusão de serviços de IA.

Etapas adicionais são necessárias para optar por não usar o Amazon Monitron. Para obter mais informações, consulte os [Termos de Serviço da AWS](#). Somente o proprietário do projeto pode optar por não usar dados pelos serviços de AWS IA.

Para desativar o uso de dados por AWS Serviços de IA

1. Abra AWS as configurações em <https://settings.aws.com>.
2. No painel de navegação principal, escolha Projeto.
3. Em Visão geral, escolha Ações e, em seguida, escolha Desativar o uso de dados pelos serviços de AWS IA.
4. Confirme sua escolha e escolha Desativar.

Solicite seu AWS Dados de ID do Builder

Warning

No momento, estamos lançando nossa nova experiência para um número limitado de clientes. Talvez você ainda não consiga acessar essa experiência.

Você pode solicitar e visualizar as informações pessoais associadas à sua ID de AWS Construtor e aos AWS aplicativos e serviços que você acessou com sua ID de AWS Construtor. Processaremos sua solicitação em até 30 dias e notificaremos você quando seus dados estiverem prontos. Enquanto sua solicitação de dados estiver pendente, você não poderá fechar seu AWS perfil. Você ainda pode fechar projetos ou a organização que possui todos os seus projetos.

Para obter mais informações sobre como exercer seus direitos de titular de dados, inclusive para informações pessoais fornecidas em relação a outros AWS sites, aplicativos, produtos, serviços, eventos e experiências, consulte [AWS Privacidade](#).

Como solicitar seus dados

1. Abra AWS as configurações em <https://settings.aws.com>.
2. No painel de navegação principal, escolha Gerenciar perfil.
3. Escolha Gerenciar perfil.

Você será redirecionado para o seu perfil AWS Builder ID.

4. Selecione Privacidade e dados.
5. Escolha solicitar seus dados de ID do Builder ou seus AWS dados.

Uma mensagem de confirmação verde aparece na parte superior da página informando que recebemos sua solicitação e a concluiremos em 30 dias.

- Quando você receber um e-mail nosso informando que a solicitação foi processada, volte para a página Privacidade e dados do seu perfil de ID do AWS Construtor. Escolha o botão recém-disponível Baixar arquivo ZIP com seus dados.

Enquanto sua solicitação de dados estiver pendente, você não poderá excluir seu AWS Builder ID.

Crie um projeto em AWS Configurações

Warning

No momento, estamos lançando nossa nova experiência para um número limitado de clientes. Talvez você ainda não consiga acessar essa experiência.

Um projeto contém um único Conta da AWS em que você cria AWS recursos. Um projeto também inclui configurações para compartilhamento com outros colaboradores. Os AWS recursos que você cria devem representar um aplicativo ou um conjunto de casos de uso relacionados. Um projeto pode abranger os ambientes de desenvolvimento e produção do seu aplicativo. Por exemplo, você pode criar um projeto chamado Livraria que contém recursos para um aplicativo de livraria, incluindo um banco de dados, recursos computacionais e armazenamento.

Você pode compartilhar esse projeto com outros membros da equipe e eles podem criar e gerenciar recursos para o aplicativo de livraria.

Cada projeto tem seus próprios controles de custo com base nos recursos da conta. Se você estiver usando o plano pago, poderá configurar um limite de gastos nas AWS Configurações para cada projeto. Para obter mais informações, consulte [Crie um limite de gastos em AWS Configurações](#). Como proprietário do projeto, você é responsável pelas faturas mensais de encargos de uso e taxas recorrentes.

Considerações para criar um projeto

- Você pode acessar projetos que não são de sua propriedade como membro da equipe.
- Cada nome de projeto deve ser exclusivo para seus projetos. Projetos pertencentes a outros membros da equipe podem ter o mesmo nome.

- Os nomes dos projetos podem conter os seguintes caracteres válidos: a-z A-Z, 0-9 e pontos (.).
- Ao criar seu projeto, AWS atribua-o a uma região — Leste dos EUA (Ohio) (), Europa (Estocolmo - east-2) () ou Ásia-Pacífico (Sydney - north-1) (ap-southeast-2) — com base no país em seu endereço de contato — Estados Unidos da América, Europa ou Ásia-Pacífico. Todos os recursos regionais que você criar serão hospedados nessa região. Para obter mais informações, consulte [Regiões da AWS para seus projetos](#).

Para criar um projeto

Para criar um projeto

1. Abra AWS as Configurações em <https://settings.aws.com>.
2. No painel de navegação principal, escolha Projeto.
3. Escolha Criar projeto.
4. Em Nome do projeto, insira um nome descritivo para seu projeto.

Esse nome é compartilhado com os membros da equipe quando você os convida para colaborar.

5. Escolha Criar.

Leva alguns segundos para criar seu projeto. Quando seu projeto estiver disponível, você poderá escolher o projeto e acessá-lo Console de gerenciamento da AWS para começar a construir.

Se você já configurou sua ferramenta de codificação de IA para interagir com a sua Conta da AWS, você pode solicitar que ela crie recursos em seu novo projeto.

Use os exemplos de instruções da sua ferramenta de codificação de IA para começar:

What is the Region for my project *test project*?

Create a hello world Lambda function in my project *test project*.

Create an S3 bucket in my project *test project*.

Regiões da AWS para seus projetos

Warning

No momento, estamos lançando nossa nova experiência para um número limitado de clientes. Talvez você ainda não consiga acessar essa experiência.

Ao criar seu projeto, AWS atribua-o a uma região — Leste dos EUA (Ohio) (), Europa (Estocolmo - east-2) () ou Ásia-Pacífico (Sydney - north-1) (ap-southeast-2) — com base no país em seu endereço de contato — Estados Unidos, Europa ou Ásia-Pacífico. Todos os recursos regionais que você criar serão hospedados nessa região.

A seguir estão as considerações sobre os selecionados Região da AWS para sua conta:

- Se você alterar suas informações de contato nas AWS Configurações, a região selecionada não mudará. Se você precisar acessar uma região específica, use Inscrever-se em AWS (avançado). Você também pode ativar recursos avançados para sua conta para selecionar diferentes regiões.
- AWS pode introduzir outras regiões suportadas, mas elas só estarão disponíveis para novas inscrições. Para ver as últimas regiões suportadas em 18 de agosto de 2026, consulte as tabelas abaixo. Se você já tem um projeto, pode encontrar a região selecionada em [AWS Configurações](#).
- Os serviços globais estão disponíveis com seu projeto. Esses serviços são acessados por meio de uma única região que pode ser diferente da sua região de origem. Para obter mais informações, consulte [AWS Fault Isolation Boundaries](#). Além disso, existem alguns serviços que estão disponíveis em regiões específicas. No Console de gerenciamento da AWS, você pode visualizar esses serviços em determinadas regiões, mas retornará à região selecionada ao navegar para um serviço diferente.
- Se você usa o Amazon Bedrock, pode usar APIs que não criam recursos em todos os comerciais Regiões da AWS que estão habilitados por padrão.
- Se você usar CloudFront, certos recursos que criariam recursos fora da região selecionada não estarão disponíveis. Isso inclui o uso AWS WAF com CloudFront.
- Alguns CloudTrail eventos envolvendo os serviços globais são registrados na região em que o serviço global opera. Você tem acesso a esses eventos.
- AWS WAF e o Amazon CloudWatch Logs estão disponíveis no Leste dos EUA (Norte da Virgínia) (us-east-1).

Você pode descobrir qual é a região selecionada para todos os projetos em sua conta usando AWS as Configurações. No Console de gerenciamento da AWS, a maioria dos consoles de serviço está hospedada na região em que você está, incluindo Bedrock e SageMaker. Se você já analisou um console de serviço de um serviço global, o console encaminha automaticamente todas as suas chamadas de API para a região apropriada para o serviço global.

Encontre o selecionado Região da AWS para seus projetos

Como prática recomendada, recomendamos que você sempre confirme o Região da AWS para seu projeto antes de criar qualquer AWS recurso.

Para encontrar o selecionado Região da AWS para seus projetos

1. Abra AWS as configurações em <https://settings.aws.com>.
2. No painel de navegação principal, escolha Projeto.
3. Na seção Visão geral, escolha Informações adicionais.

Nessa visualização, você também pode encontrar o Conta da AWS ID associado ao seu projeto.

4. Em Região, você verá em que Região da AWS seu projeto foi provisionado.

Quando você cria AWS recursos regionais em qualquer um dos seus projetos, os nomes de recursos da Amazon desses recursos incluirão isso Região da AWS.

Países onde os recursos regionais são provisionados no Leste dos EUA (Ohio) (**us-east-2**)

Nome do país	Código do país
Antígua e Barbuda	AG
Argentina	AR
Bahamas	BS
Barbados	BB
Belize	BZ

Nome do país	Código do país
Bolívia	BO
Brasil	BR
Canadá	CA
Chile	CL
Colômbia	CO
Costa Rica	CR
Dominica	DM
República Dominicana	DO
Equador	EC
El Salvador	SV
Granada	GD
Guatemala	GT
Guiana	GY
Haiti	HT
Honduras	HN
Jamaica	JM
México	MX
Nicarágua	NI
Panamá	PA
Paraguai	PY

Nome do país	Código do país
Peru	PE
São Cristóvão e Nevis	KN
Santa Lúcia	LC
São Vicente e Granadinas	VC
Suriname	SR
Trinidad e Tobago	TT
Estados Unidos	EUA
Uruguai	UY
Venezuela	VE
Anguila	AI
Aruba	AW
Bermudas	BM
Bonaire, Santo Eustáquio e Saba	BQ
Ilhas Virgens Britânicas	VG
Ilhas Cayman	KY
Curaçau	CW
Ilhas Falkland	FK
Guiana Francesa	GF
Guadalupe	GP
Martinica	MQ

Nome do país	Código do país
Montserrat	MS
Porto Rico	PR
São Bartolomeu	BL
São Martinho	MF
Saint Pierre e Miquelon	PM
Sint Maarten	SX
Ilhas Turcas e Caicos	TC
U.S. Ilhas Virgens	VI

Países onde os recursos regionais são provisionados na Ásia-Pacífico (Sydney) (**ap-southeast-2**)

Nome do país	Código do país
Afeganistão	AF
Austrália	AU
Bangladesh	BD
Butão	BT
Brunei	BN
Camboja	KG
China	CN
Timor Leste () Timor-Leste	TL

Nome do país	Código do país
Fiji	FJ
Hong Kong	HK
Índia	IN
Indonésia	ID
Japão	JP
Cazaquistão	KZ
Quiribati	KI
Quirguistão	KG
Laos	LA
Macau	MO
Malásia	MY
Ilhas Maldivas	MV
Ilhas Marshall	MH
Micronésia	FM
Mongólia	MN
Mianmar	MM
Nauru	NR
Nepal	NP
Nova Zelândia	NZ
Paquistão	PK

Nome do país	Código do país
Palau	PW
Papua Nova Guiné	PG
Filipinas	PH
Samoa	WS
Cingapura	SG
Ilhas Salomão	SB
Coreia do Sul	KR
Sri Lanka	LK
Taiwan	TW
Tajiquistão	TJ
Tailândia	TH
Tonga	TO
Turcomenistão	TM
Tuvalu	TV
Uzbequistão	UZ
Vanuatu	VU
Vietnã	VN
Samoa Americana	AS
Ilha Christmas	CX
Ilhas Cocos (Keeling)	CC

Nome do país	Código do país
Ilhas Cook	CK
Polinésia Francesa	PF
Guam	GU
Ilha e McDonald Ilhas Heard	HM
Nova Caledônia	NC
Niue	NU
Ilha Norfolk	NF
Ilhas Marianas do Norte	MP
Ilhas Pitcairn	PN
Toquelau	TK
U.S. Ilhas Menores Distantes	UM
Wallis e Futuna	WF

Países onde os recursos regionais são provisionados na Europa (Estocolmo) (eu-north-1)

Nome do país	Código do país
Albânia	AL
Argélia	DZ
Andorra	AD
Angola	AO

Nome do país	Código do país
Armênia	AM
Áustria	AT
Azerbaijão	AZ
Bahrein	BH
Bielorrússia	BY
Bélgica	BE
Benin	BJ
Bósnia e Herzegovina	BA
Botsuana	BW
Bulgária	BG
Burkina Faso	BF
Burundi	BI
Cabo Verde	CV
Camarões	CM
República Centro-Africana	CF
Chade	TD
Comores	KM
Congo (Brazzaville)	CG
Congo (RDC)	CD
Costa do Marfim	CI

Nome do país	Código do país
Croácia	HR
Chipre	CY
República Tcheca	CZ
Dinamarca	DK
Djibuti	DJ
Egito	EG
Guiné Equatorial	GQ
Eritreia	ER
Estônia	EE
Essuatíni	SZ
Etiópia	ET
Finlândia	FI
França	FR
Gabão	GA
Gâmbia	GM
Geórgia	GE
Alemanha	DE
Gana	GH
Grécia	GR
Guiné	GN

Nome do país	Código do país
Guinea-Bissau	GW
Hungria	HU
Islândia	IS
Iraque	IQ
Irlanda	IE
Israel	IL
Itália	IT
Jordânia	JO
Quênia	KE
Kosovo	XK
Kuwait	KW
Letônia	LV
Líbano	LB
Lesoto	LS
Libéria	LR
Líbia	LY
Liechtenstein	LI
Lituânia	LT
Luxemburgo	LU
Madagascar	MG

Nome do país	Código do país
Malawi	MW
Mali	ML
Malta	MT
Mauritânia	MR
Ilhas Maurício	MU
Moldávia	MD
Mônaco	MC
Montenegro	ME
Marrocos	MA
Moçambique	MZ
Namíbia	NA
Holanda	NL
Níger	NE
Nigéria	NG
Macedônia do Norte	MK
Noruega	NO
Omã	OM
Palestina	PS
Polônia	PL
Portugal	PT

Nome do país	Código do país
Catar	QA
Romênia	RO
Rússia	RU
Ruanda	RW
São Marinho	SM
São Tomé e Príncipe	ST
Arábia Saudita	SA
Senegal	SN
Sérvia	RS
Seichelles	SC
Serra Leoa	SL
Eslováquia	SK
Eslovênia	SI
Somália	SO
África do Sul	ZA
Sudão do Sul	SS
Espanha	ES
Suécia	SE
Suíça	CH
Tanzânia	TZ

Nome do país	Código do país
Togo	TG
Tunísia	TN
Turquia	TR
Uganda	UG
Ucrânia	UA
Emirados Árabes Unidos	AE
Reino Unido	GB
Cidade do Vaticano	VA
Iêmen	YE
Zâmbia	ZM
Zimbábue	ZW
Ilhas Åland	AX
Antártida	AQ
Ilha Bouvet	BV
Território Britânico do Oceano Índico	IO
Ilhas Faroe	FO
Territórios Franceses do Sul	TF
Gibraltar	GI
Groenlândia	GL
Guernsey	GG

Nome do país	Código do país
Ilha de Man	IM
Jérsei	JE
Mayotte	YT
Reunião	RE
Santa Helena	SH
Ilhas Geórgia do Sul e Sandwich do Sul	GS
Svalbard e Jan Mayen	SJ
Saara Ocidental	EH

Políticas gerenciadas para sua organização

Warning

No momento, estamos lançando nossa nova experiência para um número limitado de clientes. Talvez você ainda não consiga acessar essa experiência.

Quando você usa nossa nova AWS experiência, AWS gerencia as políticas de gerenciamento da organização, incluindo as políticas de controle de recursos (RCPs) e as políticas de controle de serviços (SCPs). Esses controles de proteção evitam que o proprietário do projeto ou membro da equipe execute ações que inibam os padrões AWS pré-configurados definidos para ajudá-lo a criar e desenvolver rapidamente.

Políticas de controle de serviços para projetos

A seguir está uma política de controle de serviço para todos os usuários em um projeto e não pode ser alterada:

```
{  
  "Version" : "2012-10-17",
```



```

"Statement" : [
  {
    "Sid" : "BlockOrgEscape",
    "Effect" : "Deny",
    "Action" : [
      "account:CloseAccount",
      "organizations:AcceptHandshake",
      "organizations:LeaveOrganization",
      "sso:CreateInstance"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "ProtectManagedRoles",
    "Effect" : "Deny",
    "Action" : [
      "iam:AttachRolePolicy",
      "iam:CreateRole",
      "iam>DeleteRole",
      "iam>DeleteRolePermissionsBoundary",
      "iam>DeleteRolePolicy",
      "iam:DetachRolePolicy",
      "iam:PutRolePermissionsBoundary",
      "iam:PutRolePolicy",
      "iam:TagRole",
      "iam:UntagRole",
      "iam:UpdateAssumeRolePolicy",
      "iam:UpdateRole"
    ],
    "Resource" : "arn:*:iam::*:role/managed/*",
    "Condition" : {
      "StringNotLike" : {
        "aws:PrincipalArn" : "arn:*:iam::*:role/managed/
AWSManagedAccountManagementAccessRole"
      }
    }
  }
]
}

```

Essa política não é removida quando você ativa recursos avançados. Para obter mais informações, consulte [Ativar avançado AWS recursos](#).

Depois de ativar os recursos avançados, essa política permanece vinculada à raiz da sua organização, portanto, ela se aplica a todas as contas de membros, incluindo contas que você cria ou convida posteriormente.

Além disso, aplicamos a seguinte política de controle de serviço a todos os usuários em um projeto para restringir determinadas modificações em seu projeto que não são suportadas ou devem ser concluídas em AWS Configurações:

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "BlockAccountManagementAPIs",
      "Effect" : "Deny",
      "Action" : [
        "account:AcceptPrimaryEmailUpdate",
        "account:DeleteAlternateContact",
        "account:DisableRegion",
        "account:EnableRegion",
        "account:GetAlternateContact",
        "account:GetContactInformation",
        "account:GetGovCloudAccountInformation",
        "account:GetRegionOptStatus",
        "account:PutAccountName",
        "account:PutAlternateContact",
        "account:PutContactInformation",
        "account:StartPrimaryEmailUpdate"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DenyBillingOperations",
      "Effect" : "Deny",
      "Action" : "billing:*",
      "Resource" : "*"
    },
    {
      "Sid" : "DenyNotificationContactsOperations",
      "Effect" : "Deny",
      "Action" : "notifications-contacts:*",
      "Resource" : "*"
    }
  ],
  {
```

```

    "Sid" : "DenyRestrictedNotificationOperations",
    "Effect" : "Deny",
    "Action" : [
        "notifications:AssociateChannel",
        "notifications:AssociateManagedNotificationAccountContact",
        "notifications:AssociateManagedNotificationAdditionalChannel",
        "notifications:AssociateOrganizationalUnit",
        "notifications:CreateEventRule",
        "notifications:CreateNotificationConfiguration",
        "notifications>DeleteEventRule",
        "notifications>DeleteNotificationConfiguration",
        "notifications:DeregisterNotificationHub",
        "notifications:DisableNotificationsAccessForOrganization",
        "notifications:DisassociateChannel",
        "notifications:DisassociateManagedNotificationAccountContact",
        "notifications:DisassociateManagedNotificationAdditionalChannel",
        "notifications:DisassociateOrganizationalUnit",
        "notifications:EnableNotificationsAccessForOrganization",
        "notifications:GetEventRule",
        "notifications:GetFeatureOptInStatus",
        "notifications:GetNotificationConfiguration",
        "notifications:GetNotificationEvent",
        "notifications:GetNotificationsAccessForOrganization",
        "notifications:ListChannels",
        "notifications:ListEventRules",
        "notifications:ListManagedNotificationChannelAssociations",
        "notifications:ListMemberAccounts",
        "notifications:ListNotificationConfigurations",
        "notifications:ListNotificationEvents",
        "notifications:ListNotificationHubs",
        "notifications:ListOrganizationalUnits",
        "notifications:ListTagsForResource",
        "notifications:PutFeatureOptInStatus",
        "notifications:RegisterNotificationHub",
        "notifications:TagResource",
        "notifications:UntagResource",
        "notifications:UpdateEventRule",
        "notifications:UpdateNotificationConfiguration"
    ],
    "Resource" : "*"
},
{
    "Sid" : "DenyRoleManagerDisablement",
    "Effect" : "Deny",

```

```

    "Action" : "iam:PutAccountProperties",
    "Resource" : "*",
    "Condition" : {
      "ForAnyValue:StringEquals" : {
        "iam:AccountPropertyNamespaces" : "RoleManager"
      }
    }
  }
]
}

```

Essa política é removida quando você ativa recursos avançados. Para obter mais informações, consulte [Ativar avançado AWS recursos](#).

A remoção dessa política não permite que você atualize o endereço de e-mail do usuário raiz de uma conta do projeto. Para obter mais informações, consulte [Contas do projeto depois de ativar os recursos avançados](#).

Além disso, também aplicamos a seguinte política de controle de serviço a todos os usuários em um projeto Regiões da AWS para restringir a fim de permitir o suporte a serviços particionais, dependendo do seu *selected-region*:

```

{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "UsEast1Partitonal",
      "Effect" : "Deny",
      "NotAction" : [
        "account:*",
        "acm:*",
        "activate:*",
        "artifact:*",
        "aws-marketplace:*",
        "bedrock-mantle:CallWithBearerToken",
        "bedrock-mantle:CreateInference",
        "bedrock-mantle:GetInference",
        "bedrock-mantle:GetModel",
        "bedrock-mantle:ListModels",
        "bedrock:ApplyGuardrail",
        "bedrock:CountTokens",
        "bedrock:GetFoundationModel",
        "bedrock:GetFoundationModelAvailability",

```

```
"bedrock:GetInferenceProfile",
"bedrock:InvokeModel",
"bedrock:InvokeModelWithResponseStream",
"bedrock:ListFoundationModels",
"bedrock:ListInferenceProfiles",
"budgets:*",
"ce:*",
"chatbot:*",
"cloudfront-keyvaluestore:*",
"cloudfront:*",
"cloudshell:*",
"cloudtrail:LookupEvents",
"cloudwatch:BatchGet*",
"cloudwatch:Describe*",
"cloudwatch:GenerateQuery",
"cloudwatch:Get*",
"cloudwatch:List*",
"consoleapp:*",
"cost-optimization-hub:*",
"ec2:DescribeRegions",
"ecr-public:*",
"freetier:*",
"health:*",
"iam:*",
"identitystore-auth:*",
"identitystore:*",
"invoicing:*",
"kms:CreateGrant",
"kms:Decrypt",
"kms:DescribeKey",
"kms:ListAliases",
"lightsail:AttachCertificateToDistribution",
"lightsail:CreateCertificate",
"lightsail:CreateContactMethod",
"lightsail:CreateDistribution",
"lightsail:CreateDomain",
"lightsail:CreateDomainEntry",
"lightsail>DeleteAlarm",
"lightsail>DeleteCertificate",
"lightsail>DeleteContactMethod",
"lightsail>DeleteDistribution",
"lightsail>DeleteDomain",
"lightsail>DeleteDomainEntry",
"lightsail:DetachCertificateFromDistribution",
```

```

    "lightsail:Get*",
    "lightsail:IsVpcPeered",
    "lightsail:PutAlarm",
    "lightsail:ResetDistributionCache",
    "lightsail:SendContactMethodVerification",
    "lightsail:SetIpAddressType",
    "lightsail:TagResource",
    "lightsail:TestAlarm",
    "lightsail:UntagResource",
    "lightsail:UpdateDistribution",
    "lightsail:UpdateDistributionBundle",
    "lightsail:UpdateDomainEntry",
    "logs:*",
    "managedblockchain-query:*",
    "managedblockchain:*",
    "mapcredits:*",
    "notifications:GetManagedNotificationConfiguration",
    "notifications:GetManagedNotificationEvent",
    "notifications:ListManagedNotificationChildEvents",
    "notifications:ListManagedNotificationConfigurations",
    "notifications:ListManagedNotificationEvents",
    "organizations:*",
    "pricing:*",
    "q:*",
    "route53:*",
    "route53domains:*",
    "route53globalresolver:*",
    "s3:GetBucketLocation",
    "s3:ListAllMyBuckets",
    "servicequotas:*",
    "signin:*",
    "sso-directory:*",
    "sso-oauth:*",
    "sso:*",
    "sts:*",
    "support:*",
    "tax:*",
    "trustedadvisor:*",
    "uxc:*",
    "waf:*",
    "wafv2:*"
  ],
  "Resource" : "*",
  "Condition" : {

```

```

        "StringEquals" : {
            "aws:RequestedRegion" : "us-east-1"
        }
    },
    {
        "Sid" : "DenyUsEast1WafResourceAssociation",
        "Effect" : "Deny",
        "Action" : [
            "wafv2:AssociateWebACL",
            "wafv2:DisassociateWebACL",
            "wafv2:GetWebACLForResource",
            "wafv2:ListResourcesForWebACL"
        ],
        "Resource" : "*",
        "Condition" : {
            "StringEquals" : {
                "aws:RequestedRegion" : "us-east-1"
            }
        }
    },
    {
        "Sid" : "UsWest2Partitional",
        "Effect" : "Deny",
        "NotAction" : [
            "bedrock-mantle:CallWithBearerToken",
            "bedrock-mantle:CreateInference",
            "bedrock-mantle:GetInference",
            "bedrock-mantle:GetModel",
            "bedrock-mantle:ListModels",
            "bedrock:ApplyGuardrail",
            "bedrock:CountTokens",
            "bedrock:GetFoundationModel",
            "bedrock:GetFoundationModelAvailability",
            "bedrock:GetInferenceProfile",
            "bedrock:InvokeModel",
            "bedrock:InvokeModelWithResponseStream",
            "bedrock:ListFoundationModels",
            "bedrock:ListInferenceProfiles",
            "cloudshell:*",
            "cloudtrail:LookupEvents",
            "health:*",
            "identitystore-auth:*",
            "identitystore:*"
        ]
    }
}

```

```

    "kms:Decrypt",
    "kms:DescribeKey",
    "kms:ListAliases",
    "networkmanager-chat:*",
    "networkmanager:*",
    "route53-recovery-cluster:*",
    "route53-recovery-control-config:*",
    "route53-recovery-readiness:*",
    "servicequotas:*",
    "sso-directory:*",
    "sso-oauth:*",
    "sso:*",
    "support:*",
    "trustedadvisor:*",
    "uxc:*"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "aws:RequestedRegion" : "us-west-2"
    }
  }
},
{
  "Sid" : "RegionFloor",
  "Effect" : "Deny",
  "NotAction" : [
    "bedrock-mantle:CallWithBearerToken",
    "bedrock-mantle:CreateInference",
    "bedrock-mantle:GetInference",
    "bedrock-mantle:GetModel",
    "bedrock-mantle:ListModels",
    "bedrock:ApplyGuardrail",
    "bedrock:CountTokens",
    "bedrock:GetFoundationModel",
    "bedrock:GetFoundationModelAvailability",
    "bedrock:GetInferenceProfile",
    "bedrock:InvokeModel",
    "bedrock:InvokeModelWithResponseStream",
    "bedrock:ListFoundationModels",
    "bedrock:ListInferenceProfiles"
  ],
  "Resource" : "*",
  "Condition" : {

```



```

    "StringNotEquals" : {
      "aws:RequestedRegion" : [
        "unspecified",
        "us-east-1",
        "selected-region",
        "us-west-2"
      ]
    }
  }
}
]
}

```

Depois de ativar os recursos avançados, a seguinte política de controle de serviço é aplicada à sua conta:

```

{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "UsEast1Partitional",
      "Effect" : "Deny",
      "NotAction" : [
        "a4b:*",
        "access-analyzer:*",
        "account-access:*",
        "account:*",
        "acm:*",
        "activate:*",
        "artifact:*",
        "aws-marketplace-management:*",
        "aws-marketplace:*",
        "aws-portal:*",
        "bedrock-mantle:CallWithBearerToken",
        "bedrock-mantle:CreateInference",
        "bedrock-mantle:GetInference",
        "bedrock-mantle:GetModel",
        "bedrock-mantle:ListModels",
        "bedrock:ApplyGuardrail",
        "bedrock:CountTokens",
        "bedrock:GetFoundationModel",
        "bedrock:GetFoundationModelAvailability",
        "bedrock:GetInferenceProfile",

```

```
"bedrock:InvokeModel",
"bedrock:InvokeModelWithResponseStream",
"bedrock:ListFoundationModels",
"bedrock:ListInferenceProfiles",
"billing:*",
"billingconductor:*",
"budgets:*",
"builderid:*",
"ce:*",
"chatbot:*",
"chime:*",
"cloudfront-keyvaluestore:*",
"cloudfront:*",
"cloudshell:*",
"cloudtrail:LookupEvents",
"cloudwatch:BatchGet*",
"cloudwatch:Describe*",
"cloudwatch:GenerateQuery",
"cloudwatch:Get*",
"cloudwatch:List*",
"compute-optimizer:*",
"config:*",
"consoleapp:*",
"consolidatedbilling:*",
"cost-optimization-hub:*",
"cur:*",
"datapipeline:GetAccountLimits",
"devicefarm:*",
"directconnect:*",
"ec2:DescribeRegions",
"ec2:DescribeTransitGateways",
"ec2:DescribeVpnGateways",
"ecr-public:*",
"fms:*",
"freetier:*",
"globalaccelerator:*",
"health:*",
"iam:*",
"identitystore-auth:*",
"identitystore:*",
"importexport:*",
" invoicing:*",
"iq:*",
"kms:*",
```

```
"license-manager:ListReceivedLicenses",
"lightsail:AttachCertificateToDistribution",
"lightsail:CreateCertificate",
"lightsail:CreateContactMethod",
"lightsail:CreateDistribution",
"lightsail:CreateDomain",
"lightsail:CreateDomainEntry",
"lightsail>DeleteAlarm",
"lightsail>DeleteCertificate",
"lightsail>DeleteContactMethod",
"lightsail>DeleteDistribution",
"lightsail>DeleteDomain",
"lightsail>DeleteDomainEntry",
"lightsail:DetachCertificateFromDistribution",
"lightsail:Get*",
"lightsail:IsVpcPeered",
"lightsail:PutAlarm",
"lightsail:ResetDistributionCache",
"lightsail:SendContactMethodVerification",
"lightsail:SetIpAddressType",
"lightsail:TagResource",
"lightsail:TestAlarm",
"lightsail:UntagResource",
"lightsail:UpdateDistribution",
"lightsail:UpdateDistributionBundle",
"lightsail:UpdateDomainEntry",
"logs:*",
"managedblockchain-query:*",
"managedblockchain:*",
"mapcredits:*",
"mobileanalytics:*",
"networkmanager:*",
"notifications-contacts:*",
"notifications:*",
"organizations:*",
"payments:*",
"pricing:*",
"q:*",
"quicksight:DescribeAccountSubscription",
"resource-explorer-2:*",
"route53-recovery-cluster:*",
"route53-recovery-control-config:*",
"route53-recovery-readiness:*",
"route53:*,
```

```

    "route53domains:*",
    "route53globalresolver:*",
    "s3:CreateMultiRegionAccessPoint",
    "s3:DeleteMultiRegionAccessPoint",
    "s3:DescribeMultiRegionAccessPointOperation",
    "s3:GetAccountPublicAccessBlock",
    "s3:GetBucketLocation",
    "s3:GetBucketPolicyStatus",
    "s3:GetBucketPublicAccessBlock",
    "s3:GetMultiRegionAccessPoint",
    "s3:GetMultiRegionAccessPointPolicy",
    "s3:GetMultiRegionAccessPointPolicyStatus",
    "s3:GetStorageLensConfiguration",
    "s3:GetStorageLensDashboard",
    "s3:ListAllMyBuckets",
    "s3:ListMultiRegionAccessPoints",
    "s3:ListStorageLensConfigurations",
    "s3:PutAccountPublicAccessBlock",
    "s3:PutMultiRegionAccessPointPolicy",
    "savingsplans:*",
    "servicequotas:*",
    "shield:*",
    "signin:*",
    "sso-directory:*",
    "sso-oauth:*",
    "sso:*",
    "sts:*",
    "support:*",
    "supportapp:*",
    "supportplans:*",
    "sustainability:*",
    "tag:GetResources",
    "tax:*",
    "trustedadvisor:*",
    "uxc:*",
    "vendor-insights:ListEntitledSecurityProfiles",
    "waf-regional:*",
    "waf:*",
    "wafv2:*"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "aws:RequestedRegion" : "us-east-1"
    }
  }
}

```

```

    }
  }
},
{
  "Sid" : "UsWest2Partititional",
  "Effect" : "Deny",
  "NotAction" : [
    "bedrock-mantle:CallWithBearerToken",
    "bedrock-mantle:CreateInference",
    "bedrock-mantle:GetInference",
    "bedrock-mantle:GetModel",
    "bedrock-mantle:ListModels",
    "bedrock:ApplyGuardrail",
    "bedrock:CountTokens",
    "bedrock:GetFoundationModel",
    "bedrock:GetFoundationModelAvailability",
    "bedrock:GetInferenceProfile",
    "bedrock:InvokeModel",
    "bedrock:InvokeModelWithResponseStream",
    "bedrock:ListFoundationModels",
    "bedrock:ListInferenceProfiles",
    "cloudshell:*",
    "cloudtrail:LookupEvents",
    "health:*",
    "identitystore-auth:*",
    "identitystore:*",
    "kms:Decrypt",
    "kms:DescribeKey",
    "kms:ListAliases",
    "networkmanager-chat:*",
    "networkmanager:*",
    "route53-recovery-cluster:*",
    "route53-recovery-control-config:*",
    "route53-recovery-readiness:*",
    "servicequotas:*",
    "sso-directory:*",
    "sso-oauth:*",
    "sso:*",
    "support:*",
    "trustedadvisor:*",
    "uxc:*"
  ],
  "Resource" : "*",
  "Condition" : {

```

```
    "StringEquals" : {
      "aws:RequestedRegion" : "us-west-2"
    }
  },
  {
    "Sid" : "RegionFloor",
    "Effect" : "Deny",
    "NotAction" : [
      "bedrock-mantle:CallWithBearerToken",
      "bedrock-mantle:CreateInference",
      "bedrock-mantle:GetInference",
      "bedrock-mantle:GetModel",
      "bedrock-mantle:ListModels",
      "bedrock:ApplyGuardrail",
      "bedrock:CountTokens",
      "bedrock:GetFoundationModel",
      "bedrock:GetFoundationModelAvailability",
      "bedrock:GetInferenceProfile",
      "bedrock:InvokeModel",
      "bedrock:InvokeModelWithResponseStream",
      "bedrock:ListFoundationModels",
      "bedrock:ListInferenceProfiles"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringNotEquals" : {
        "aws:RequestedRegion" : [
          "unspecified",
          "us-east-1",
          "selected-region",
          "us-west-2"
        ]
      }
    }
  }
]
```

Políticas de controle de serviço para limites de gastos

Se você usa um limite de gastos, as seguintes políticas de controle de serviço são aplicadas ao seu projeto quando ele se aproxima do limite de gastos. Para obter mais informações sobre limites de gastos, consulte [Crie um limite de gastos em AWS Configurações](#).

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Sid": "DenyBedrockUsage",
    "Effect": "Deny",
    "Action": [
      "bedrock:ApplyGuardrail",
      "bedrock:CallWithBearerToken",
      "bedrock:InvokeAgent",
      "bedrock:InvokeAutomatedReasoningPolicy",
      "bedrock:InvokeDataAutomation",
      "bedrock:InvokeDataAutomationAsync",
      "bedrock:InvokeFlow",
      "bedrock:InvokeInlineAgent",
      "bedrock:InvokeModel",
      "bedrock:InvokeModelWithResponseStream",
      "bedrock:InvokeTool",
      "bedrock:OptimizePrompt",
      "bedrock:Retrieve",
      "bedrock:RetrieveAndGenerate",
      "bedrock:StartFlowExecution",
      "bedrock-mantle:CallWithBearerToken",
      "bedrock-mantle:CreateInference"
    ],
    "Resource": "*"
  }
}
```

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Sid": "DenyLambdaUsage",
    "Effect": "Deny",
    "Action": [
      "lambda:DeleteFunctionConcurrency",
      "lambda:InvokeAsync",
      "lambda:InvokeFunction",

```

```
    "lambda:InvokeFunctionUrl",
    "lambda:PutFunctionConcurrency"
  ],
  "Resource": "*"
}
```

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Sid": "DenySageMakerInference",
    "Effect": "Deny",
    "Action": [
      "sagemaker:InvokeEndpoint",
      "sagemaker:InvokeEndpointAsync",
      "sagemaker:InvokeEndpointWithResponseStream"
    ],
    "Resource": "*"
  }
}
```

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyCompute",
      "Effect": "Deny",
      "Action": [
        "ec2:CreateNatGateway",
        "ec2:CreateVolume",
        "ec2:CreateVpnConnection",
        "ec2:RunInstances",
        "ec2:StartInstances",
        "elasticloadbalancing:CreateLoadBalancer",
        "autoscaling:CreateAutoScalingGroup",
        "ecs:CreateService",
        "eks:CreateCluster",
        "eks:CreateNodegroup",
        "eks:CreateFargateProfile",
        "elasticbeanstalk:CreateEnvironment",
        "apprunner:CreateService",
        "apprunner:ResumeService",
        "batch:CreateComputeEnvironment",

```



```

        "elasticmapreduce:RunJobFlow",
        "appstream:CreateFleet"
    ],
    "Resource": "*"
},
{
    "Sid": "DenyLambda",
    "Effect": "Deny",
    "Action": "lambda:CreateFunction",
    "Resource": "*"
},
{
    "Sid": "DenyDatabase",
    "Effect": "Deny",
    "Action": [
        "rds:CreateDBCluster",
        "rds:CreateDBInstance",
        "rds:RestoreDBClusterFromS3",
        "rds:RestoreDBClusterFromSnapshot",
        "rds:RestoreDBClusterToPointInTime",
        "rds:RestoreDBInstanceFromDBSnapshot",
        "rds:RestoreDBInstanceFromS3",
        "rds:RestoreDBInstanceToPointInTime",
        "rds:StartDBCluster",
        "rds:StartDBInstance",
        "dynamodb:CreateTable",
        "dynamodb:CreateGlobalTable",
        "elasticache:CreateCacheCluster",
        "elasticache:CreateReplicationGroup",
        "timestream:CreateDatabase",
        "timestream:CreateTable",
        "memorydb:CreateCluster",
        "es:CreateDomain",
        "aoss:CreateCollection",
        "redshift:CreateCluster",
        "redshift:ResumeCluster",
        "redshift-serverless:CreateWorkgroup",
        "dsq:CreateCluster"
    ],
    "Resource": "*"
},
{
    "Sid": "DenyStorage",
    "Effect": "Deny",

```

```

    "Action": [
      "elasticfilesystem:CreateFileSystem",
      "datasync:CreateTask",
      "storagegateway:ActivateGateway",
      "glacier:CreateVault"
    ],
    "Resource": "*"
  },
  {
    "Sid": "DenySageMaker",
    "Effect": "Deny",
    "Action": [
      "sagemaker:CreateApp",
      "sagemaker:CreateEndpoint",
      "sagemaker:CreateNotebookInstance",
      "sagemaker:CreateProcessingJob",
      "sagemaker:CreateTrainingJob",
      "sagemaker:CreateTransformJob",
      "sagemaker:StartNotebookInstance"
    ],
    "Resource": "*"
  },
  {
    "Sid": "DenyBedrock",
    "Effect": "Deny",
    "Action": [
      "bedrock:CreateCustomModelDeployment",
      "bedrock:CreateDataAutomationProject",
      "bedrock:CreateEvaluationJob",
      "bedrock:CreateMarketplaceModelEndpoint",
      "bedrock:CreateModelCustomizationJob",
      "bedrock:CreateModelImportJob",
      "bedrock:CreateModelInvocationJob",
      "bedrock:CreateProvisionedModelThroughput",
      "bedrock-mantle:CreateCustomizedModel",
      "bedrock-mantle:CreateFineTuningJob",
      "bedrock-mantle:CreateReservation"
    ],
    "Resource": "*"
  },
  {
    "Sid": "DenyAIML",
    "Effect": "Deny",
    "Action": [

```

```

        "kendra:CreateIndex",
        "personalize:CreateSolution",
        "personalize:CreateCampaign",
        "forecast:CreatePredictor",
        "forecast:CreateForecast",
        "rekognition:CreateProject",
        "lex:CreateBot"
    ],
    "Resource": "*"
},
{
    "Sid": "DenyNetworking",
    "Effect": "Deny",
    "Action": [
        "cloudfront:CreateDistribution",
        "route53:CreateHostedZone",
        "appmesh:CreateMesh"
    ],
    "Resource": "*"
},
{
    "Sid": "DenyApiGatewayCreate",
    "Effect": "Deny",
    "Action": "apigateway:POST",
    "Resource": [
        "arn:aws:apigateway:*::/restapis",
        "arn:aws:apigateway:*::/apis"
    ]
},
{
    "Sid": "DenyMessaging",
    "Effect": "Deny",
    "Action": [
        "mq:CreateBroker",
        "kafka:CreateCluster",
        "kafka:CreateVpcConnection",
        "kinesis:CreateStream",
        "firehose:CreateDeliveryStream",
        "kinesisanalytics:CreateApplication",
        "kinesisvideo:CreateStream",
        "sns:CreateTopic",
        "sqs:CreateQueue",
        "events:CreateEventBus",
        "pipes:CreatePipe",

```

```

    "scheduler:CreateSchedule"
  ],
  "Resource": "*"
},
{
  "Sid": "DenyAnalytics",
  "Effect": "Deny",
  "Action": [
    "states:CreateStateMachine",
    "glue:CreateJob",
    "glue:CreateCrawler",
    "athena:CreateWorkGroup",
    "appsync:CreateGraphQLApi",
    "appflow:CreateFlow",
    "datazone:CreateDomain",
    "datazone:CreateProject",
    "entityresolution:CreateMatchingWorkflow",
    "datapipeline:CreatePipeline",
    "dataexchange:CreateDataSet"
  ],
  "Resource": "*"
},
{
  "Sid": "DenyDevTools",
  "Effect": "Deny",
  "Action": [
    "amplify:CreateApp",
    "amplify:CreateBranch",
    "cloud9:CreateEnvironmentEC2",
    "codebuild:CreateProject",
    "codepipeline:CreatePipeline",
    "codedeploy:CreateApplication",
    "cloudformation:CreateStack",
    "cloudformation:CreateStackSet",
    "codeartifact:CreateRepository",
    "codeartifact:CreateDomain"
  ],
  "Resource": "*"
},
{
  "Sid": "DenySecurity",
  "Effect": "Deny",
  "Action": [
    "kms:CreateKey",

```

```

        "wafv2:CreateWebACL",
        "cloudhsm:CreateCluster",
        "network-firewall:CreateFirewall",
        "secretsmanager:CreateSecret",
        "acm-pca:CreateCertificateAuthority",
        "cognito-idp:CreateUserPool",
        "cognito-identity:CreateIdentityPool",
        "ds:CreateDirectory",
        "ds:CreateMicrosoftAD",
        "fms:PutPolicy",
        "payment-cryptography:CreateKey"
    ],
    "Resource": "*"
},
{
    "Sid": "DenyMedia",
    "Effect": "Deny",
    "Action": [
        "medialive:CreateChannel",
        "mediapackage:CreateChannel",
        "mediaconnect:CreateFlow",
        "mediatailor:CreateChannel"
    ],
    "Resource": "*"
},
{
    "Sid": "DenyIoT",
    "Effect": "Deny",
    "Action": [
        "iot:CreateThing",
        "iot:CreateTopicRule",
        "iotevents:CreateDetectorModel",
        "iottwinmaker:CreateWorkspace",
        "iotsitewise:CreateAssetModel",
        "iotsitewise:CreatePortal",
        "iotfleetwise:CreateCampaign"
    ],
    "Resource": "*"
},
{
    "Sid": "DenyMisc",
    "Effect": "Deny",
    "Action": [
        "ses:CreateConfigurationSet",

```

```

    "ecr:CreateRepository",
    "aps:CreateWorkspace",
    "healthlake:CreateFHIRDatastore",
    "transfer:CreateServer",
    "managedblockchain:CreateNetwork",
    "managedblockchain:CreateMember",
    "route53-recovery-control-config:CreateCluster",
    "fis:CreateExperimentTemplate",
    "appfabric:CreateAppBundle",
    "appfabric:CreateIngestion",
    "b2bi:CreateProfile",
    "b2bi:CreateTransformer",
    "geo:CreateMap",
    "geo:CreatePlaceIndex",
    "geo:CreateTracker",
    "geo:CreateGeofenceCollection",
    "geo:CreateRouteCalculator"
  ],
  "Resource": "*"
}
]
}

```

Políticas de controle de serviço para o nível gratuito para projetos

A política de controle de serviço a seguir controla o acesso aos AWS serviços disponíveis no nível gratuito de nossa nova AWS experiência. Essa política não pode ser modificada. Para acessar serviços adicionais, atualize sua conta. Para obter mais informações, consulte [Atualize sua conta em AWS Configurações](#).

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowFreeTierServices",
      "Effect": "Deny",
      "NotAction": [
        "a2c:*",
        "access-analyzer:CheckAccessNotGranted",
        "access-analyzer:CheckNoNewAccess",
        "access-analyzer:CheckNoPublicAccess",
        "access-analyzer:ValidatePolicy",
        "account:*",

```

```
"acm:*",
"aco-automation:*",
"action-recommendations:*",
"activate:*",
"aiops:*",
"airflow-serverless:*",
"amplify:*",
"amplifybackend:*",
"amplifyuibuilder:*",
"aoss:*",
"apigateway:*",
"app-integrations:*",
"appconfig:*",
"appflow:*",
"application-autoscaling:*",
"application-signals-mcp:*",
"application-signals:*",
"application-transformation:*",
"applicationinsights:*",
"appmesh:*",
"appsync:*",
"aps:*",
"arc-zonal-shift:*",
"artifact:*",
"athena:*",
"autoscaling-plans:*",
"autoscaling:*",
"aws-external-anthropic:*",
"aws-marketplace:*",
"b2bi:*",
"backup-gateway:*",
"backup-search:*",
"backup-storage:*",
"backup:*",
"batch:*",
"bcm-pricing-calculator:*",
"bedrock-agentcore:*",
"bedrock-mantle:*",
"bedrock-websearch:*",
"bedrock:*",
"budgets:*",
"ce:*",
"chatbot:*",
"cloud9:*
```

```
"cloudformation:*",
"cloudfront-keyvaluestore:*",
"cloudfront:*",
"cloudshell:*",
"cloudtrail-data:*",
"cloudtrail:*",
"cloudwatch:*",
"codeartifact:*",
"codebuild:*",
"codecommit:*",
"codeconnections:*",
"codedeploy-commands-secure:*",
"codedeploy:*",
"codepipeline:*",
"codestar-connections:*",
"codestar-notifications:*",
"cognito-identity:*",
"cognito-idp:*",
"cognito-sync:*",
"compute-optimizer:*",
"config:*",
"consoleapp:*",
"consolidatedbilling:*",
"cost-optimization-hub:*",
"customer-verification:*",
"databrew:*",
"datapipeline:*",
"datasync:*",
"datazone:*",
"dbqms:*",
"dlm:*",
"ds-data:*",
"ds:*",
"dsql:*",
"dynamodb:*",
"ebs:*",
"ec2-instance-connect:*",
"ec2:*",
"ec2messages:*",
"ecr-public:*",
"ecr:*",
"ecs-mcp:*",
"ecs:*",
"eks-auth:*",
```



```
"eks-mcp:*",
"eks:*",
"elasticache:*",
"elasticbeanstalk:*",
"elasticfilesystem:*",
"elasticloadbalancing:*",
"entityresolution:*",
"es:*",
"events:*",
"evidently:*",
"execute-api:*",
"finops-agent:*",
"freertos:*",
"freetier:*",
"geo-maps:*",
"geo-places:*",
"geo-routes:*",
"geo:*",
"glue:*",
"groundtruthlabeling:*",
"health:*",
"iam:*",
"identitystore-auth:*",
"identitystore:*",
"imagebuilder:*",
"internetmonitor:*",
"invoicing:*",
"iot-device-tester:*",
"iot:*",
"iotdeviceadvisor:*",
"iotfleethub:*",
"iotjobsdata:*",
"iotmanagedintegrations:*",
"iotsitewise:*",
"iottwinmaker:*",
"iotwireless:*",
"kms:*",
"lakeformation:*",
"lambda:*",
"launchwizard:*",
"lex:*",
"license-manager-linux-subscriptions:*",
"license-manager-user-subscriptions:*",
"license-manager:*,
```

```
"logs:*",
"mgn:*",
"migrationhub-orchestrator:*",
"migrationhub-strategy:*",
"mpa:*",
"mq:*",
"networkflowmonitor:*",
"networkmanager-chat:*",
"networkmanager:*",
"networkmonitor:*",
"notifications-contacts:*",
"notifications:*",
"nova-act:*",
"oam:*",
"observabilityadmin:*",
"opensearch:*",
"organizations:*",
"osis:*",
"payment-cryptography:*",
"pi:*",
"pipes:*",
"polly:*",
"pricing:*",
"q:DeleteConversation",
"q:GenerateCodeFromCommands",
"q:GenerateCodeRecommendations",
"q:GetConversation",
"q:GetIdentityMetadata",
"q:GetTroubleshootingResults",
"q:ListConversations",
"q:PassRequest",
"q:SendEvent",
"q:SendMessage",
"q:StartConversation",
"q:StartTroubleshootingAnalysis",
"q:StartTroubleshootingResolutionExplanation",
"q:UpdateConversation",
"q:UpdateTroubleshootingCommandResult",
"q:UsePlugin",
"ram:*",
"rbin:*",
"rds-data:*",
"rds-db:*",
"rds:*
```

```
"rekognition:*",
"resource-explorer-2:*",
"resource-explorer:*",
"resource-groups:*",
"rhelkb:*",
"route53-recovery-cluster:*",
"route53-recovery-control-config:*",
"route53-recovery-readiness:*",
"route53:*",
"route53domains:*",
"route53globalresolver:*",
"route53profiles:*",
"route53resolver:*",
"rum:*",
"s3-object-lambda:*",
"s3:*",
"s3express:*",
"s3files:*",
"s3tables:*",
"s3vectors:*",
"sagemaker-data-science-assistant:*",
"sagemaker-geospatial:*",
"sagemaker-mlflow:*",
"sagemaker-unified-studio-mcp:*",
"sagemaker:*",
"scheduler:*",
"schemas:*",
"secretsmanager:*",
"serverlessrepo:*",
"servicecatalog:Describe*",
"servicecatalog:List*",
"servicecatalog:ProvisionProduct",
"servicecatalog:ScanProvisionedProducts",
"servicecatalog:SearchProducts",
"servicecatalog:SearchProvisionedProducts",
"servicecatalog:TerminateProvisionedProduct",
"servicecatalog:UpdateProvisionedProduct",
"servicediscovery:*",
"serviceextract:*",
"servicequotas:*",
"ses:*",
"signer:*",
"signin:*",
"sns:*",
```

```

    "sqlworkbench:*",
    "sqs:*",
    "ssm-contacts:*",
    "ssm-guiconnect:*",
    "ssm-incidents:*",
    "ssm-quicksetup:*",
    "ssm-sap:*",
    "ssm:*",
    "ssmmessages:*",
    "sso-directory:*",
    "sso-oauth:*",
    "sso:*",
    "states:*",
    "sts:*",
    "support:*",
    "swf:*",
    "synthetics:*",
    "tag:*",
    "tax:*",
    "timestream-influxdb:*",
    "ts:*",
    "uxc:*",
    "verifiedpermissions:*",
    "vpce:*",
    "waf-regional:*",
    "waf:*",
    "wafv2:*",
    "wellarchitected:*",
    "xray:*"
  ],
  "Resource": "*"
},
{
  "Sid": "DenyEC2CapacityBlock",
  "Effect": "Deny",
  "Action": ["ec2:PurchaseCapacityBlock", "ec2:PurchaseCapacityBlockExtension"],
  "Resource": "*"
},
{
  "Sid": "DenyRestrictedAgreements",
  "Effect": "Deny",
  "Action": ["artifact:AcceptAgreement", "artifact:AcceptNdaForAgreement"],
  "Resource": [
    "arn:aws:artifact::agreement/agreement-9c1kBcYznTkcpRIm",

```

```

        "arn:aws:artifact::agreement/agreement-y03aUwMAEorHtqjv",
        "arn:aws:artifact::agreement/agreement-bexgr7sjvXAW4Gxu",
        "arn:aws:artifact::agreement/agreement-HZTdNwJuq0KLReXC"
    ]
},
{
    "Sid": "DenyDocDB",
    "Effect": "Deny",
    "Action": ["rds:CreateDBCluster", "rds:CreateDBInstance"],
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "rds:DatabaseEngine": ["docdb"]
        }
    }
},
{
    "Sid": "DenyCloudWAN",
    "Effect": "Deny",
    "Action": [
        "networkmanager:CreateCoreNetwork",
        "networkmanager:CreateConnectAttachment",
        "networkmanager:CreateConnectPeer",
        "networkmanager:CreateVpcAttachment",
        "networkmanager:CreateSiteToSiteVpnAttachment",
        "networkmanager:CreateTransitGatewayPeering",
        "networkmanager:CreateDirectConnectGatewayAttachment",
        "networkmanager:PutCoreNetworkPolicy",
        "networkmanager:ExecuteCoreNetworkChangeSet"
    ],
    "Resource": "*"
},
{
    "Sid": "DenyTransitGatewayAndVPN",
    "Effect": "Deny",
    "Action": [
        "ec2:CreateTransitGateway",
        "ec2:CreateTransitGatewayVpcAttachment",
        "ec2:CreateTransitGatewayConnect",
        "ec2:CreateTransitGatewayConnectPeer",
        "ec2:CreateTransitGatewayMulticastDomain",
        "ec2:CreateTransitGatewayPeeringAttachment",
        "ec2:CreateTransitGatewayPolicyTable",
        "ec2:CreateTransitGatewayPrefixListReference",

```

```

        "ec2:CreateTransitGatewayRoute",
        "ec2:CreateTransitGatewayRouteTable",
        "ec2:CreateTransitGatewayRouteTableAnnouncement",
        "ec2:CreateClientVpnEndpoint",
        "ec2:CreateClientVpnRoute",
        "ec2:AuthorizeClientVpnIngress",
        "ec2:AssociateClientVpnTargetNetwork",
        "ec2:CreateVpnConnection",
        "ec2:CreateVpnConnectionRoute",
        "ec2:CreateVpnGateway",
        "ec2:CreateCustomerGateway"
    ],
    "Resource": "*"
},
{
    "Sid": "DenySageMakerGroundTruth",
    "Effect": "Deny",
    "Action": [
        "sagemaker:CreateLabelingJob",
        "sagemaker:CreateWorkteam",
        "sagemaker:CreateWorkforce",
        "sagemaker:CreateHumanTaskUi"
    ],
    "Resource": "*"
},
{
    "Sid": "DenyGlacierStorageClasses",
    "Effect": "Deny",
    "Action": ["s3:PutObject"],
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "s3:x-amz-storage-class": ["DEEP_ARCHIVE", "GLACIER"]
        }
    }
},
{
    "Sid": "DenyEC2Fleet",
    "Effect": "Deny",
    "Action": ["ec2:CreateFleet"],
    "Resource": "*"
},
{
    "Sid": "DenyEC2BYOLAndLicenseConfigurations",

```

```

    "Effect": "Deny",
    "Action": ["ec2:RunInstances", "ec2:StartInstances"],
    "Resource": "arn:aws:ec2:*:*:instance/*",
    "Condition": {
      "StringEquals": {
        "ec2:Tenancy": "host"
      }
    }
  },
  {
    "Sid": "DenyEC2InstanceStoreRootDevice",
    "Effect": "Deny",
    "Action": ["ec2:RunInstances"],
    "Resource": "arn:aws:ec2:*:*:instance/*",
    "Condition": {
      "StringEquals": {
        "ec2:RootDeviceType": "instance-store"
      }
    }
  },
  {
    "Sid": "DenyLicenseManagerAssociation",
    "Effect": "Deny",
    "Action": ["license-manager:CreateLicenseConfiguration"],
    "Resource": "*"
  },
  {
    "Sid": "DenyIAMRestrictedActions",
    "Effect": "Deny",
    "Action": [
      "iam:*Alias*",
      "iam:*Organizations*",
      "iam:*Provider*",
      "iam:SetSecurityTokenServicePreferences",
      "iam:*LoginProfile*",
      "iam:CreateGroup",
      "iam:AttachGroupPolicy",
      "iam:AddUserToGroup",
      "iam:PutGroupPolicy",
      "iam:UpdateGroup",
      "iam:UpdateServerCertificate",
      "iam:UpdateSigningCertificate",
      "iam:UploadServerCertificate",
      "iam:UploadSigningCertificate",
    ]
  }
}

```

```

        "iam:TagServerCertificate",
        "iam:UntagServerCertificate"
    ],
    "Resource": "*"
},
{
    "Sid": "DenySSOCreateInstance",
    "Effect": "Deny",
    "Action": ["sso:CreateInstance"],
    "Resource": "*"
},
{
    "Sid": "DenyRequestSpotInstances",
    "Effect": "Deny",
    "Action": ["ec2:RequestSpotInstances"],
    "Resource": "*"
},
{
    "Sid": "DenySpotMarketType",
    "Effect": "Deny",
    "Action": ["ec2:RunInstances"],
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "ec2:InstanceMarketType": "spot"
        }
    }
},
{
    "Sid": "DenyReservedInstanceAndCapacityPurchases",
    "Effect": "Deny",
    "Action": [
        "athena:CreateCapacityReservation",
        "cloudfront:CreateSavingsPlan",
        "dynamodb:PurchaseReservedCapacityOfferings",
        "ec2:AllocateHosts",
        "ec2:CreateCapacityReservation",
        "ec2:CreateCapacityReservationBySplitting",
        "ec2:CreateCapacityReservationCancellationQuote",
        "ec2:CreateCapacityReservationFleet",
        "ec2:PurchaseHostReservation",
        "ec2:PurchaseReservedInstancesOffering",
        "ec2:PurchaseScheduledInstances",
        "elasticache:PurchaseReservedCacheNodesOffering",
    ]
}

```



```

        "es:PurchaseReservedElasticsearchInstanceOffering",
        "es:PurchaseReservedInstanceOffering",
        "glacier:PurchaseProvisionedCapacity",
        "memorydb:PurchaseReservedNodesOffering",
        "rds:PurchaseReservedDBInstancesOffering",
        "redshift:AcceptReservedNodeExchange",
        "redshift:PurchaseReservedNodeOffering",
        "sagemaker:CreateReservedCapacity",
        "savingsplans:CreateSavingsPlan"
    ],
    "Resource": "*"
  },
  {
    "Sid": "DenyExportableCertificateRequests",
    "Effect": "Deny",
    "Action": ["acm:RequestCertificate"],
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "acm:AllowExport": "true"
      }
    }
  }
]
}

```

Políticas de controle de serviço para o plano pago para projetos

A política de controle de serviço a seguir controla o acesso aos AWS serviços disponíveis no plano pago de nossa nova AWS experiência. Essa política não pode ser modificada. Para acessar serviços adicionais, ative os recursos avançados. Para obter mais informações, consulte [Ativar avançado AWS recursos](#).

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowPaidTierServices",
      "Effect": "Deny",
      "NotAction": [
        "a2c:*",
        "access-analyzer:CheckAccessNotGranted",
        "access-analyzer:CheckNoNewAccess",

```

```
"access-analyzer:CheckNoPublicAccess",
"access-analyzer:ValidatePolicy",
"account:*",
"acm:*",
"aco-automation:*",
"action-recommendations:*",
"activate:*",
"aidevops:*",
"aiops:*",
"airflow-serverless:*",
"amplify:*",
"amplifybackend:*",
"amplifyuibuilder:*",
"aoss:*",
"apigateway:*",
"app-integrations:*",
"appconfig:*",
"appfabric:*",
"appflow:*",
"application-autoscaling:*",
"application-signals-mcp:*",
"application-signals:*",
"application-transformation:*",
"applicationinsights:*",
"appmesh:*",
"appsync:*",
"aps:*",
"arc-zonal-shift:*",
"artifact:*",
"athena:*",
"autoscaling-plans:*",
"autoscaling:*",
"aws-external-anthropic:*",
"aws-marketplace:*",
"b2bi:*",
"backup-gateway:*",
"backup-search:*",
"backup-storage:*",
"backup:*",
"batch:*",
"bcm-pricing-calculator:*",
"bedrock-agentcore:*",
"bedrock-mantle:*",
"bedrock-websearch:*,
```

```
"bedrock:*",
"budgets:*",
"ce:*",
"chatbot:*",
"cloud9:*",
"cloudformation:*",
"cloudfront-keyvaluestore:*",
"cloudfront:*",
"cloudshell:*",
"cloudtrail-data:*",
"cloudtrail:*",
"cloudwatch:*",
"codeartifact:*",
"codebuild:*",
"codecommit:*",
"codeconnections:*",
"codedeploy-commands-secure:*",
"codedeploy:*",
"codeguru-profiler:*",
"codeguru-reviewer:*",
"codeguru-security:*",
"codepipeline:*",
"codestar-connections:*",
"codestar-notifications:*",
"cognito-identity:*",
"cognito-idp:*",
"cognito-sync:*",
"compute-optimizer:*",
"config:*",
"consoleapp:*",
"consolidatedbilling:*",
"cost-optimization-hub:*",
"customer-verification:*",
"databrew:*",
"dataexchange:*",
"datapipeline:*",
"datasync:*",
"datazone:*",
"dbqms:*",
"devops-guru:*",
"dlm:*",
"docdb-elastic:*",
"ds-data:*",
"ds:*,
```

```
"dsq1:*",
"dynamodb:*",
"ebs:*",
"ec2-instance-connect:*",
"ec2:*",
"ec2messages:*",
"ecr-public:*",
"ecr:*",
"ecs-mcp:*",
"ecs:*",
"eks-auth:*",
"eks-mcp:*",
"eks:*",
"elasticache:*",
"elasticbeanstalk:*",
"elasticfilesystem:*",
"elasticloadbalancing:*",
"elasticmapreduce:*",
"emr-containers:*",
"emr-serverless:*",
"entityresolution:*",
"es:*",
"events:*",
"evidently:*",
"execute-api:*",
"finops-agent:*",
"firehose:*",
"fis:*",
"fms:*",
"forecast:*",
"freertos:*",
"freetier:*",
"geo-maps:*",
"geo-places:*",
"geo-routes:*",
"geo:*",
"glacier:*",
"glue:*",
"groundtruthlabeling:*",
"health:*",
"iam:*",
"identitystore-auth:*",
"identitystore:*",
"imagebuilder:*
```

```
"internetmonitor:*",
"invoicing:*",
"iot-device-tester:*",
"iot:*",
"iotdeviceadvisor:*",
"iotfleethub:*",
"iotjobsdata:*",
"iotmanagedintegrations:*",
"iotsitewise:*",
"iottwinmaker:*",
"iotwireless:*",
"kafka-cluster:*",
"kafka:*",
"kafkaconnect:*",
"kinesis:*",
"kinesisanalytics:*",
"kinesisvideo:*",
"kms:*",
"lakeformation:*",
"lambda:*",
"launchwizard:*",
"lex:*",
"license-manager-linux-subscriptions:*",
"license-manager-user-subscriptions:*",
"license-manager:*",
"logs:*",
"managedblockchain-query:*",
"managedblockchain:*",
"mapcredits:*",
"memorydb:*",
"mgn:*",
"migrationhub-orchestrator:*",
"migrationhub-strategy:*",
"mpa:*",
"mq:*",
"neptune-db:*",
"neptune-graph:*",
"network-firewall:*",
"networkflowmonitor:*",
"networkmanager-chat:*",
"networkmanager:*",
"networkmonitor:*",
"notifications-contacts:*",
"notifications:*,
```

```
"nova-act:*",
"oam:*",
"observabilityadmin:*",
"opensearch:*",
"organizations:*",
"osis:*",
"payment-cryptography:*",
"personalize:*",
"pi:*",
"pipes:*",
"polly:*",
"pricing:*",
"q:DeleteConversation",
"q:GenerateCodeFromCommands",
"q:GenerateCodeRecommendations",
"q:GetConversation",
"q:GetIdentityMetadata",
"q:GetTroubleshootingResults",
"q:ListConversations",
"q:PassRequest",
"q:SendEvent",
"q:SendMessage",
"q:StartConversation",
"q:StartTroubleshootingAnalysis",
"q:StartTroubleshootingResolutionExplanation",
"q:UpdateConversation",
"q:UpdateTroubleshootingCommandResult",
"q:UsePlugin",
"ram:*",
"rbin:*",
"rds-data:*",
"rds-db:*",
"rds:*",
"redshift-data:*",
"redshift-serverless:*",
"redshift:*",
"rekognition:*",
"resource-explorer-2:*",
"resource-explorer:*",
"resource-groups:*",
"rhelkb:*",
"route53-recovery-cluster:*",
"route53-recovery-control-config:*",
"route53-recovery-readiness:*",
```

```
"route53:*",
"route53domains:*",
"route53globalresolver:*",
"route53profiles:*",
"route53resolver:*",
"rum:*",
"s3-object-lambda:*",
"s3:*",
"s3express:*",
"s3files:*",
"s3tables:*",
"s3vectors:*",
"sagemaker-data-science-assistant:*",
"sagemaker-geospatial:*",
"sagemaker-mlflow:*",
"sagemaker-unified-studio-mcp:*",
"sagemaker:*",
"scheduler:*",
"schemas:*",
"secretsmanager:*",
"securityagent:*",
"serverlessrepo:*",
"servicecatalog:Describe*",
"servicecatalog:List*",
"servicecatalog:ProvisionProduct",
"servicecatalog:ScanProvisionedProducts",
"servicecatalog:SearchProducts",
"servicecatalog:SearchProvisionedProducts",
"servicecatalog:TerminateProvisionedProduct",
"servicecatalog:UpdateProvisionedProduct",
"servicediscovery:*",
"serviceextract:*",
"servicequotas:*",
"ses:*",
"signer:*",
"signin:*",
"sms-voice:*",
"sns:*",
"social-messaging:*",
"sqlworkbench:*",
"sqs:*",
"ssm-contacts:*",
"ssm-guiconnect:*",
"ssm-incidents:*
```

```

    "ssm-quicksetup:*",
    "ssm-sap:*",
    "ssm:*",
    "ssmmessages:*",
    "sso-directory:*",
    "sso-oauth:*",
    "sso:*",
    "states:*",
    "storagegateway:*",
    "sts:*",
    "support:*",
    "swf:*",
    "synthetics:*",
    "tag:*",
    "tax:*",
    "textract:*",
    "timestream-influxdb:*",
    "timestream:*",
    "transcribe:*",
    "translate:*",
    "ts:*",
    "uxc:*",
    "verifiedpermissions:*",
    "vpce:*",
    "waf-regional:*",
    "waf:*",
    "wafv2:*",
    "wellarchitected:*",
    "xray:*"
  ],
  "Resource": "*"
},
{
  "Sid": "DenyEC2CapacityBlock",
  "Effect": "Deny",
  "Action": ["ec2:PurchaseCapacityBlock", "ec2:PurchaseCapacityBlockExtension"],
  "Resource": "*"
},
{
  "Sid": "DenyRestrictedAgreements",
  "Effect": "Deny",
  "Action": ["artifact:AcceptAgreement", "artifact:AcceptNdaForAgreement"],
  "Resource": [
    "arn:aws:artifact::agreement/agreement-9c1kBcYznTkcpRIm",

```



```

        "arn:aws:artifact::agreement/agreement-y03aUwMAEorHtqjv",
        "arn:aws:artifact::agreement/agreement-bexgr7sjvXAW4Gxu",
        "arn:aws:artifact::agreement/agreement-HZTdNwJuqOKLReXC"
    ]
},
{
    "Sid": "DenyCloudWAN",
    "Effect": "Deny",
    "Action": [
        "networkmanager:CreateCoreNetwork",
        "networkmanager:CreateConnectAttachment",
        "networkmanager:CreateConnectPeer",
        "networkmanager:CreateVpcAttachment",
        "networkmanager:CreateSiteToSiteVpnAttachment",
        "networkmanager:CreateTransitGatewayPeering",
        "networkmanager:CreateDirectConnectGatewayAttachment",
        "networkmanager:PutCoreNetworkPolicy",
        "networkmanager:ExecuteCoreNetworkChangeSet"
    ],
    "Resource": "*"
},
{
    "Sid": "DenyTransitGatewayAndVPN",
    "Effect": "Deny",
    "Action": [
        "ec2:CreateTransitGateway",
        "ec2:CreateTransitGatewayVpcAttachment",
        "ec2:CreateTransitGatewayConnect",
        "ec2:CreateTransitGatewayConnectPeer",
        "ec2:CreateTransitGatewayMulticastDomain",
        "ec2:CreateTransitGatewayPeeringAttachment",
        "ec2:CreateTransitGatewayPolicyTable",
        "ec2:CreateTransitGatewayPrefixListReference",
        "ec2:CreateTransitGatewayRoute",
        "ec2:CreateTransitGatewayRouteTable",
        "ec2:CreateTransitGatewayRouteTableAnnouncement",
        "ec2:CreateClientVpnEndpoint",
        "ec2:CreateClientVpnRoute",
        "ec2:AuthorizeClientVpnIngress",
        "ec2:AssociateClientVpnTargetNetwork",
        "ec2:CreateVpnConnection",
        "ec2:CreateVpnConnectionRoute",
        "ec2:CreateVpnGateway",
        "ec2:CreateCustomerGateway"
    ]
}

```

```

    ],
    "Resource": "*"
  },
  {
    "Sid": "DenySageMakerGroundTruth",
    "Effect": "Deny",
    "Action": [
      "sagemaker:CreateLabelingJob",
      "sagemaker:CreateWorkteam",
      "sagemaker:CreateWorkforce",
      "sagemaker:CreateHumanTaskUi"
    ],
    "Resource": "*"
  },
  {
    "Sid": "DenyEC2Fleet",
    "Effect": "Deny",
    "Action": ["ec2:CreateFleet"],
    "Resource": "*"
  },
  {
    "Sid": "DenyEC2BYOLAndLicenseConfigurations",
    "Effect": "Deny",
    "Action": ["ec2:RunInstances", "ec2:StartInstances"],
    "Resource": "arn:aws:ec2:*:*:instance/*",
    "Condition": {
      "StringEquals": {
        "ec2:Tenancy": "host"
      }
    }
  },
  {
    "Sid": "DenyEC2InstanceStoreRootDevice",
    "Effect": "Deny",
    "Action": ["ec2:RunInstances"],
    "Resource": "arn:aws:ec2:*:*:instance/*",
    "Condition": {
      "StringEquals": {
        "ec2:RootDeviceType": "instance-store"
      }
    }
  },
  {
    "Sid": "DenyLicenseManagerAssociation",

```

```
"Effect": "Deny",
"Action": ["license-manager:CreateLicenseConfiguration"],
"Resource": "*"
},
{
  "Sid": "DenyIAMRestrictedActions",
  "Effect": "Deny",
  "Action": [
    "iam:*Alias*",
    "iam:*Organizations*",
    "iam:*Provider*",
    "iam:SetSecurityTokenServicePreferences",
    "iam:*LoginProfile*",
    "iam:CreateGroup",
    "iam:AttachGroupPolicy",
    "iam:AddUserToGroup",
    "iam:PutGroupPolicy",
    "iam:UpdateGroup",
    "iam:UpdateServerCertificate",
    "iam:UpdateSigningCertificate",
    "iam:UploadServerCertificate",
    "iam:UploadSigningCertificate",
    "iam:TagServerCertificate",
    "iam:UntagServerCertificate"
  ],
  "Resource": "*"
},
{
  "Sid": "DenySSOCreateInstance",
  "Effect": "Deny",
  "Action": ["sso:CreateInstance"],
  "Resource": "*"
},
{
  "Sid": "DenyRequestSpotInstances",
  "Effect": "Deny",
  "Action": ["ec2:RequestSpotInstances"],
  "Resource": "*"
},
{
  "Sid": "DenySpotMarketType",
  "Effect": "Deny",
  "Action": ["ec2:RunInstances"],
  "Resource": "*",
```

```

    "Condition": {
      "StringEquals": {
        "ec2:InstanceMarketType": "spot"
      }
    },
    {
      "Sid": "DenyReservedInstanceAndCapacityPurchases",
      "Effect": "Deny",
      "Action": [
        "athena:CreateCapacityReservation",
        "cloudfront:CreateSavingsPlan",
        "dynamodb:PurchaseReservedCapacityOfferings",
        "ec2:AllocateHosts",
        "ec2:CreateCapacityReservation",
        "ec2:CreateCapacityReservationBySplitting",
        "ec2:CreateCapacityReservationCancellationQuote",
        "ec2:CreateCapacityReservationFleet",
        "ec2:PurchaseHostReservation",
        "ec2:PurchaseReservedInstancesOffering",
        "ec2:PurchaseScheduledInstances",
        "elasticache:PurchaseReservedCacheNodesOffering",
        "es:PurchaseReservedElasticsearchInstanceOffering",
        "es:PurchaseReservedInstanceOffering",
        "glacier:PurchaseProvisionedCapacity",
        "memorydb:PurchaseReservedNodesOffering",
        "rds:PurchaseReservedDBInstancesOffering",
        "redshift:AcceptReservedNodeExchange",
        "redshift:PurchaseReservedNodeOffering",
        "sagemaker:CreateReservedCapacity",
        "savingsplans:CreateSavingsPlan"
      ],
      "Resource": "*"
    },
    {
      "Sid": "DenyExportableCertificateRequests",
      "Effect": "Deny",
      "Action": ["acm:RequestCertificate"],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "acm:AllowExport": "true"
        }
      }
    }
  ]
}

```

```
}  
]  
}
```

Políticas de controle de recursos para projetos

A seguir está a política de controle de recursos para os [recursos do projeto](#). Esta política não pode ser modificada:

```
{  
  "Version" : "2012-10-17",  
  "Statement" : [  
    {  
      "Sid" : "DenyAnyoneOutsideMyOrgAndAWS",  
      "Effect" : "Deny",  
      "Principal" : "*",  
      "Action" : [  
        "aoss:*",  
        "appconfig:*",  
        "appstream:*",  
        "autoscaling:*",  
        "codebuild:*",  
        "codecommit:*",  
        "cognito-identity:*",  
        "cognito-idp:*",  
        "comprehend:*",  
        "comprehendmedical:*",  
        "dax:*",  
        "dynamodb:*",  
        "ecr:*",  
        "health:*",  
        "kinesisvideo:*",  
        "kms:*",  
        "logs:*",  
        "s3:*",  
        "secretsmanager:*",  
        "sqs:*",  
        "sts:*",  
        "support:*",  
        "textract:*",  
        "transcribe:*",  
        "translate:"  
      ],  
    },  
  ],  
}
```

```

    "Resource" : "*",
    "Condition" : {
      "BoolIfExists" : {
        "aws:PrincipalIsAWSService" : "false"
      },
      "Null" : {
        "aws:PrincipalARN" : "false"
      },
      "StringNotEqualsIfExists" : {
        "aws:PrincipalOrgID" : "${aws:ResourceOrgID}"
      }
    }
  },
  {
    "Sid" : "DenyAWSWhenItsNotMyOrgsSourceAccount",
    "Effect" : "Deny",
    "Principal" : "*",
    "Action" : [
      "aoss:*",
      "appconfig:*",
      "appstream:*",
      "autoscaling:*",
      "codebuild:*",
      "codecommit:*",
      "cognito-identity:*",
      "cognito-idp:*",
      "comprehend:*",
      "comprehendmedical:*",
      "dax:*",
      "dynamodb:*",
      "ecr:*",
      "health:*",
      "kinesisvideo:*",
      "kms:*",
      "logs:*",
      "s3:*",
      "secretsmanager:*",
      "sqs:*",
      "sts:*",
      "support:*",
      "textract:*",
      "transcribe:*",
      "translate:*"
    ]
  },

```

```
"Resource" : "*",
"Condition" : {
  "Null" : {
    "aws:SourceAccount" : "false"
  },
  "StringNotEquals" : {
    "aws:SourceOrgID" : "${aws:ResourceOrgID}"
  }
}
}
```

Alternar entre projetos

Warning

No momento, estamos lançando nossa nova experiência para um número limitado de clientes. Talvez você ainda não consiga acessar essa experiência.

Você só pode gerenciar AWS recursos para um projeto por vez. Você sempre pode saber em qual projeto você está com base no nome no canto superior direito do AWS console.

Alternar entre projetos para sessões ativas a partir do Console de gerenciamento da AWS

Para alternar entre projetos para sessões ativas do Console de gerenciamento da AWS

1. Abra a [Console de gerenciamento da AWS](#).
2. Escolha o nome do seu projeto no canto superior direito do Console de gerenciamento da AWS.
3. Escolha Switch project.
4. Em Sessões ativas, escolha uma sessão ativa. Uma sessão ativa é uma sessão que foi conectada por até 12 horas. O horário da sessão ativa não pode ser alterado.
5. Você será redirecionado para a página inicial do AWS console do seu novo projeto.

Alternar entre projetos em AWS Configurações

Para alternar entre projetos no AWS Configurações

1. Abra AWS as configurações em <https://settings.aws.com>.
2. No painel de navegação principal, escolha o projeto que você deseja acessar.
3. Na barra de navegação no canto superior direito, escolha Criar e gerenciar a infraestrutura de nuvem.

Você será redirecionado de volta Console de gerenciamento da AWS para o seu novo projeto.

Alternar entre projetos a partir do Console de gerenciamento da AWS

Para alternar entre projetos do Console de gerenciamento da AWS

1. Abra a [Console de gerenciamento da AWS](#).
2. Escolha Gerenciar projetos.
3. Em AWS Configurações, escolha o projeto que você deseja acessar.
4. Na barra de navegação no canto superior direito, escolha Criar e gerenciar infraestrutura em nuvem.

Você será redirecionado de volta Console de gerenciamento da AWS para o seu novo projeto.

Convide membros da equipe para colaborar em AWS Configurações

Warning

No momento, estamos lançando nossa nova experiência para um número limitado de clientes. Talvez você ainda não consiga acessar essa experiência.

Você pode dar aos membros da equipe acesso aos seus projetos. Quando você compartilha um projeto com um membro da equipe, você não pode controlar a quais AWS serviços ele tem acesso. Você e o membro da equipe têm acesso de administrador ao projeto. Isso significa que o membro da equipe tem permissões para acessar todos os AWS serviços disponíveis para seu projeto. Isso inclui

a criação de controles de acesso para serviços e aplicativos. No entanto, eles não têm permissão para realizar ações administrativas ou financeiras, como excluir seu projeto ou modificar um limite de gastos. Para ver qual membro da equipe modificou um AWS serviço, consulte [Monitore seu projeto usando AWS CloudTrail](#).

Nas AWS Configurações, você e os membros da sua equipe têm diferentes níveis de acesso. Para ver a política AWS gerenciada que é aplicada a um membro da equipe, consulte [AWSManagedSettingsReadOnlyAccess](#). Para ver a política AWS gerenciada que é aplicada ao proprietário do projeto, consulte [AWSManagedSettingsAdminAccess](#).

Considere o seguinte ao adicionar um membro da equipe ao seu projeto.

Considerações para os membros da equipe

Um membro da equipe pode realizar as seguintes ações:

- Visualize, crie, edite, exclua e modifique AWS recursos em um projeto.
- AWS Configurações de acesso.
- Veja os limites de gastos.
- Solicite um aumento de cota para um AWS serviço.

Um membro da equipe não pode realizar as seguintes ações:

- Saia de um projeto.
- Execute qualquer ação raiz. Para obter mais informações, consulte [AWS ações para proprietários de projetos](#).
- Convide membros da equipe para projetos.
- Gerencie as permissões de qualquer membro da equipe.
- Remova qualquer membro da equipe de um projeto.
- Altere o nome de um projeto.
- Configure ou atualize as formas de pagamento.
- Visualize ou atualize os detalhes de cobrança, incluindo endereço ou número de telefone.
- Visualize ou atualize as informações fiscais.
- Faça o upgrade do nível gratuito para o plano pago.
- Defina ou modifique os limites de gastos por projeto.

- Veja as tendências de custo de cada projeto.
- Veja AWS os gastos totais em todos os projetos.
- Visualize e resgate créditos promocionais de nível não gratuito.
- Veja os créditos restantes e as datas de vencimento de todos os tipos de crédito.
- Veja o histórico de crédito completo, incluindo créditos ganhos, aplicados e expirados.
- Veja como os créditos se aplicam em todos os projetos.
- Veja o saldo pendente.
- Execute pagamentos para AWS.
- Baixe faturas ou visualize transações anteriores.
- Verifique se as AWS cobranças estão corretas, incluindo os créditos aplicados.
- Receba comunicações de cobrança no nível da conta de gerenciamento.
- Obtenha ajuda com problemas de cobrança no nível da organização.
- Solicite um aumento de cota para cotas de contas e faturamento.

Como os membros da equipe acessam seu AWS recursos

Nossa nova AWS experiência cria uma função vinculada ao serviço para a organização que contém todos os seus projetos que você não pode modificar. Essa função verifica periodicamente se os registros internos dos membros da sua equipe permanecem sincronizados com os membros reais da equipe.

O perfil vinculado ao serviço `AWSServiceRoleForAccountAccessManager` confia nos seguintes serviços para aceitar o perfil:

- `account-access.amazonaws.com`

A política de permissões de função chamada `AccountAccessManagerServiceRolePolicy` permite que o gerente de acesso à conta conclua as seguintes ações nos recursos especificados:

- Ação: `organizations:ListAccounts,organizations:ListAWSServiceAccessForOrganizations,organizations:DescribeAccount` em `"arn:aws:organizations::*:account/o-*/*"`

Para obter mais informações, consulte [AWS Account Access Manager](#).

Convide membros da equipe para colaborar em AWS Configurações

Para convidar membros da equipe, você envia um convite da página Equipe nas AWS Configurações. Os membros da equipe têm 14 dias para aceitar o convite. Os membros da equipe devem criar um ID do builder AWS para acessar seu projeto. Eles podem fazer isso usando o Sign up for AWS (novo).

Convide membros da equipe para colaborar em AWS Configurações

1. Abra AWS as configurações em <https://settings.aws.com>.
2. No painel de navegação principal, escolha Equipe.
3. Escolha Convidar novo membro da equipe.
4. Em E-mail, insira um endereço de e-mail ou uma lista de endereços de e-mail. Separe os endereços de e-mail com vírgulas (,) ou ponto e vírgula (;).
5. Escolha um ou mais projetos para compartilhar com seus novos membros da equipe.
6. Selecione Enviar convite.

Se os membros da sua equipe não receberem o convite, peça que verifiquem suas pastas de spam e lixeira.

Convide um membro da equipe para um projeto em AWS Configurações

Warning

No momento, estamos lançando nossa nova experiência para um número limitado de clientes. Talvez você ainda não consiga acessar essa experiência.

Você pode convidar um membro da equipe para acessar um projeto. Para obter informações sobre o que os membros da equipe podem fazer em um projeto, consulte [Convide membros da equipe para colaborar em AWS Configurações](#).

Para convidar um membro da equipe para um projeto

1. Abra AWS as Configurações em <https://settings.aws.com>.

2. No painel de navegação principal, escolha o projeto que você deseja acessar.
3. Para Membros, escolha Convidar novo membro da equipe.
4. Em E-mail, insira um endereço de e-mail ou uma lista de endereços de e-mail. Separe os endereços de e-mail com vírgulas (,) ou ponto e vírgula (;).
5. Escolha um projeto para compartilhar com os novos membros da equipe.
6. Selecione Enviar convite.

Se os membros da sua equipe não receberem o convite, peça que verifiquem as pastas de spam e lixo.

Remover um membro da equipe de um projeto no AWS Configurações

Warning

No momento, estamos lançando nossa nova experiência para um número limitado de clientes. Talvez você ainda não consiga acessar essa experiência.

Você pode remover um membro da equipe de um projeto a qualquer momento. Os membros da sua equipe não podem fazer isso sozinhos. Quando você remove um membro da equipe, ele não terá mais acesso a esse projeto. Todos os recursos que seu membro da equipe criou permanecem em seu projeto e você deve gerenciá-los.

Remover um membro da equipe de um projeto

1. Abra AWS as configurações em <https://settings.aws.com>.
2. No painel de navegação principal, escolha o projeto que você deseja acessar.
3. Na guia Membros, selecione o membro com o qual você deseja remover do projeto e escolha Remover.
4. Confirme sua escolha e escolha Remover.

O membro da equipe ainda faz parte da sua equipe e você pode adicioná-lo a outros projetos. Para remover completamente um membro da equipe das AWS Configurações, consulte [Remover um membro da equipe em AWS Configurações](#).

Remover um membro da equipe em AWS Configurações

Warning

No momento, estamos lançando nossa nova experiência para um número limitado de clientes. Talvez você ainda não consiga acessar essa experiência.

Você pode usar a página Equipe para remover um membro da equipe de todos os projetos. Eles perderão automaticamente o acesso a qualquer projeto. Todos os recursos criados pelo membro da equipe não serão excluídos.

Para remover um membro da equipe

1. Abra AWS as configurações em <https://settings.aws.com>.
2. No painel de navegação principal, escolha Equipe.
3. Marque a caixa de seleção do membro da equipe que você deseja remover.
4. Escolha Remover .
5. Confirme sua escolha e escolha Remover.

Revogar um convite para um membro da equipe em AWS Configurações

Warning

No momento, estamos lançando nossa nova experiência para um número limitado de clientes. Talvez você ainda não consiga acessar essa experiência.

Você pode revogar um convite pendente. O convite permanecerá nas AWS Configurações por 14 dias. Quando você revoga um convite pendente, o link de acesso no e-mail de convite será desativado. Você não pode revogar um convite aceito, em vez disso, remover o membro da equipe. Para obter mais informações, consulte [Remover um membro da equipe em AWS Configurações](#).

Para revogar um convite

1. Abra AWS as configurações em <https://settings.aws.com>.
2. No painel de navegação principal, escolha Equipe.
3. Marque a caixa de seleção do membro da equipe que tem um convite pendente.
4. Escolha Revogar.
5. Confirme sua escolha e escolha Revogar convite.

Reenvie um convite para um membro da equipe em AWS Configurações

Warning

No momento, estamos lançando nossa nova experiência para um número limitado de clientes. Talvez você ainda não consiga acessar essa experiência.

Você pode reenviar a um membro da equipe um convite revogado, expirado ou recusado. Quando você reenvia um convite, o membro da sua equipe recebe um novo e-mail com uma data de validade de 14 dias a partir do reenvio do convite.

Para reenviar um convite

1. Abra AWS as configurações em <https://settings.aws.com>.
2. No painel de navegação principal, escolha Equipe.
3. Marque a caixa de seleção para o membro da equipe que tem um convite revogado, expirado ou recusado.
4. Escolha Reenviar.
5. Confirme sua escolha e escolha Reenviar convite.

Atualize sua conta em AWS Configurações

Warning

No momento, estamos lançando nossa nova experiência para um número limitado de clientes. Talvez você ainda não consiga acessar essa experiência.

Quando você se inscreve no Sign up for AWS (novo), suas contas estão no nível gratuito. No nível gratuito, você recebe um crédito de inscrição de USD \$100 e ganha até \$100 em créditos adicionais. Quando você ficar sem créditos ou tiver uma conta com mais de 6 meses, deverá fazer o upgrade para um plano pago. Você também pode fazer o upgrade para um plano pago a qualquer momento. Ao fazer o upgrade para um plano pago, você tem acesso aos serviços listados em [Serviços da AWS incluído no plano pago do nosso novo AWS experiência](#).

Considerações para atualizar sua conta

Considere o seguinte ao fazer o upgrade para um plano pago:

- Você não pode atualizar projetos individuais. Todos os seus projetos são atualizados quando você atualiza sua conta.
- Ao fazer o upgrade, você terá acesso aos serviços Always Free e às ofertas de teste de curto prazo.
- Você está qualificado para outros créditos e descontos promocionais.
- Você deve pagar por cobranças que excedam o saldo do crédito.
- Você pode criar um limite de gastos para definir o máximo que pagará por mês por um projeto. Para obter mais informações, consulte [Crie um limite de gastos em AWS Configurações](#).
- Você não pode designar nenhum projeto como compatível com HIPAA ou SEC.
- Sua conta não fecha quando os créditos se esgotam.
- Isso não o atualiza para [Inscreva-se para AWS \(avançado\)](#). Nenhum dos recursos que são compatíveis apenas com contas criadas usando [Inscreva-se para AWS \(avançado\)](#) estará disponível quando você atualizar sua conta. No entanto, você pode fazer [Ativar avançado AWS recursos](#) isso para sua conta.
- Você não pode reverter o processo de atualização.

Atualize sua conta em AWS Configurações

Para atualizar sua conta

1. Abra AWS as configurações em <https://settings.aws.com>.
2. No painel de navegação principal, escolha **Faturamento**.
3. Escolha **Atualizar**.
4. Escolha **Começar**.
5. Adicione sua forma de pagamento.

Com base na sua localização, talvez seja necessário fornecer algumas informações fiscais.

6. Escolha **Atualizar conta**.
7. Escolha **Continuar para retornar ao prédio** ou escolha **Definir limites de gastos** para definir um limite de gastos. Para obter mais informações sobre limites de gastos, consulte [Crie um limite de gastos em AWS Configurações](#).
8. Escolha **Ir para o console**.

Seu upgrade foi concluído.

Crie um limite de gastos em AWS Configurações

Warning

No momento, estamos lançando nossa nova experiência para um número limitado de clientes. Talvez você ainda não consiga acessar essa experiência.

O que é um limite de gastos?

Os limites de gastos permitem que os desenvolvedores usem AWS com a confiança de que podem operar dentro de um orçamento previsível e controlado. Use um limite de gastos para definir o valor máximo que você pagará por mês por um projeto. Os limites de gastos são definidos no nível do projeto. Você pode ter limites de gastos em alguns de seus projetos e outros projetos sem limites de gastos.

Se seu uso em um projeto atingir seu limite, AWS pausa esse projeto, interrompendo seus recursos para que seus custos permaneçam dentro dele. Os limites de gastos foram projetados para cargas de trabalho de experimentação, aprendizado e sandbox. Eles podem ser usados em ambientes de produção quando é aceitável fazer uma breve pausa em seus recursos nos casos em que seus aplicativos incorrem em custos inesperados.

Os limites de gastos são visíveis para qualquer pessoa com acesso ao projeto, mas só podem ser gerenciados pelos proprietários do projeto. Você precisa estar em um plano pago para criar um limite de gastos. Para obter mais informações, consulte [Atualize sua conta em AWS Configurações](#).

Os limites de gastos são um tipo de [AWS orçamento](#).

Defina seu limite de gastos

Seu limite de gastos é o teto dos custos antes de impostos do seu projeto, não uma taxa. Quando você define um limite de gastos, o valor mínimo permitido é o maior de \$20 ou uma estimativa conservadora do seu gasto provável.

Por que existe um mínimo: atingir um limite de gastos é uma experiência disruptiva. Existe o mínimo para tornar improvável que variações normais em seu uso levem a atingir o limite de gastos.

Como a estimativa conservadora é calculada: a estimativa é baseada em sua atividade no mês até o momento, mas não é uma extrapolação linear estrita. AWS analisa seus gastos até o momento e os recursos que você tem atualmente em execução. AWS também usa sua atividade do mês anterior — se for alta, ela se torna a mínima.

Se você tiver muitos recursos em funcionamento: a estimativa conservadora de seus gastos prováveis será alta. Se você quiser definir um limite menor de gastos, primeiro precisará interromper esses recursos.

Se você estiver reativando um projeto pausado: a estimativa conservadora de seu gasto provável é o gasto acumulado durante o mês, mais qualquer uso que não tenha sido cobrado.

Note

Os limites de gastos excluem créditos e se aplicam às cobranças antes de impostos.

Notificações

Você receberá notificações quando os custos reais atingirem 50%, 75% e 90% do seu limite, ou quando estiver prestes a atingir ou exceder seu limite de gastos nos próximos 10 dias.

Personalize suas configurações de limite de gastos com controles de custo antecipados opcionais

Seu limite de gastos evita que sua fatura cresça além do valor definido. Se seu uso atingir esse limite, AWS pausará seus recursos para protegê-lo. Esses controles opcionais agem mais cedo e com mais cuidado, para que você fique bem abaixo do limite.

Interromper a criação de novos recursos

Cerca de 7 dias antes de você atingir seu limite, novos recursos param de ser lançados. Isso é obtido por meio da aplicação de uma política de controle de serviços gerenciada por AWS. A política de controle do serviço depende do serviço. Para ver todas as políticas de controle de serviços que podem ser aplicadas ao seu projeto, consulte [Políticas de controle de serviço para limites de gastos](#).

Todos os seus recursos que já estão em execução continuam funcionando. Na maioria dos casos, nada do que você construiu é afetado. No entanto, em alguns casos, isso pode levar a uma experiência perturbadora. Por exemplo, se você tiver ativado o auto-scaling e se as condições forem atendidas para executar essa ação, novas instâncias não serão iniciadas.

Pausar recursos ociosos

Cerca de 5 dias antes de você atingir seu limite, os recursos ociosos são pausados. Seus aplicativos ativos continuam em execução. Os recursos ociosos são pausados com base nas recomendações do Compute AWS Optimizer. Para obter mais informações, consulte [Exibir recomendações de inatividade](#).

Você também pode ver suas recomendações de recursos ociosos fazendo login em seu projeto e visualizando oportunidades de economia. Para obter mais informações, consulte [Cust Optimization Hub](#). Neste momento, como parte de sua experiência com limites de gastos, pausaremos automaticamente o EC2, o RDS e os endpoints. SageMaker

Por que pausamos uma instância do EC2: Pausamos instâncias do EC2 se o pico de utilização da CPU estiver abaixo de 5% e sua rede I/O tiver menos de 5 MB por dia nos últimos 14 dias.

Se você tiver um tipo de instância G ou P, há um critério de inatividade diferente. Os tipos de instância G ou P serão pausados se o seguinte for verdadeiro nos últimos 14 dias:

- A GPU não está funcionando ativamente durante mais de 99% do período de retrospectiva.
- O codificador de GPU não é usado durante 99% ou mais do runtime da instância.
- O uso de memória da GPU no nível da instância é inferior a 5%
- A utilização máxima da CPU é inferior a 5%.
- A utilização da rede é inferior a 5% MB/day

Por que pausamos um banco de dados RDS: pausamos o RDS para MySQL e o RDS para PostgreSQL se a instância do banco de dados não for uma réplica de leitura e tiver o seguinte nos últimos 14 dias:

- Sem conexões de banco de dados
- Baixo uso da CPU
- Baixa read/write atividade

Por que pausamos um SageMaker endpoint ocioso: pausamos SageMaker endpoints se o endpoint não teve nenhuma invocação nos últimos 14 dias.

Pausa os principais fatores de custo

Cerca de 4 dias antes de você atingir seu limite, seu maior custo com recursos ativos é pausado. Isso pode ser uma experiência disruptiva. No momento, selecionamos os recursos desses cinco serviços: EC2, RDS, Lambda, Bedrock e SageMaker. Esse controle opcional pode impedir que você incorra em custos se tiver uma Lambda descontrolada ou um pico inesperado de Bedrock.

O que acontece se você atingir seu limite

AWS pausa seu projeto e interrompe todos os recursos. Seus dados serão preservados.

Para reativar seu projeto, aumente seu limite de gastos AWS nas Configurações. Após a reativação, alguns recursos talvez precisem ser reiniciados manualmente.

 Important

Se você não realizar nenhuma ação dentro de 90 dias após a pausa do projeto, excluirá AWS permanentemente os dados do projeto.

Outras coisas importantes a serem observadas

- Se você usa o Amazon Route 53, você só pode comprar um domínio a cada 24 horas. Você deve garantir que os custos do domínio estejam dentro dos limites de gastos, caso contrário, sua compra de domínio não será concluída. Nesses casos, você deve aumentar os limites de gastos antes de fazer uma compra.
- Você pode aplicar limites de gastos a até 10 projetos.

Crie um limite de gastos em AWS Configurações

Para criar um limite de gastos em AWS Configurações

1. Abra AWS as Configurações em <https://settings.aws.com>.
2. No painel de navegação principal, escolha Faturamento.
3. Em Custo por projeto, em Limite de gastos, escolha Definir limite para um projeto.
4. Você pode escolher o limite de gastos recomendado ou um limite personalizado.
5. Se você escolher um limite personalizado, insira o valor personalizado.
6. Escolha Definir limite de gastos.
7. Para personalizar seu limite de gastos com controles de custo antecipados, você pode selecionar Interromper o lançamento de novos recursos, Pausar recursos ociosos ou Pausar os principais fatores de custo.
8. Escolha Salvar controles de custos antecipados.

O limite de gastos entrará em vigor imediatamente.

Atualizar um limite de gastos em AWS Configurações

Warning

No momento, estamos lançando nossa nova experiência para um número limitado de clientes. Talvez você ainda não consiga acessar essa experiência.

O proprietário do projeto pode atualizar um limite de gastos nas AWS Configurações a qualquer momento. Você pode aumentar ou diminuir seu limite de gastos ou alterar os controles de custo antecipados opcionais. Se AWS bloqueou o lançamento de novos recursos ou pausou recursos porque você está se aproximando do limite, você pode aumentar seu limite de gastos. Se seu projeto foi pausado porque você atingiu seu limite, aumente seu limite de gastos para reativar seu projeto. Para obter mais informações sobre como os limites de gastos funcionam, consulte [Crie um limite de gastos em AWS Configurações](#).

Atualizar um limite de gastos em AWS Configurações

Para atualizar um limite de gastos

1. Abra AWS as configurações em <https://settings.aws.com>.
2. No painel de navegação principal, escolha **Faturamento**.
3. Em **Custo por projeto**, em **Limite de gastos**, escolha o ícone de lápis.
4. Em **Limite de gastos mensais (USD)**, insira um novo limite de gastos.

Fornecemos uma recomendação com base em seus gastos atuais.

5. Para modificar quais proteções você deseja em seu projeto, selecione **Interromper novos lançamentos de recursos**, **Pausar recursos ociosos** ou **Pausar os principais fatores de custo**.
6. Escolha **Salvar configurações**.

As mudanças no limite de gastos entrarão em vigor imediatamente.

Remova um limite de gastos em AWS Configurações

Warning

No momento, estamos lançando nossa nova experiência para um número limitado de clientes. Talvez você ainda não consiga acessar essa experiência.

O proprietário do projeto pode remover um limite de gastos nas AWS Configurações a qualquer momento. Quando você remove um limite de gastos, AWS não monitora mais seus custos nem assume nenhum controle antecipado de custos em seu projeto. Para obter mais informações sobre como os limites de gastos funcionam, consulte [Crie um limite de gastos em AWS Configurações](#).

Remova um limite de gastos em AWS Configurações

Para remover um limite de gastos

1. Abra AWS as configurações em <https://settings.aws.com>.
2. No painel de navegação principal, escolha Faturamento.
3. Em Custo por projeto, em Limite de gastos, escolha o ícone de lápis.
4. Escolha Remover limite.
5. Confirme sua escolha e escolha Remover.

Seu limite de gastos será removido imediatamente.

Nível gratuito em nosso novo AWS experiência

Warning

No momento, estamos lançando nossa nova experiência para um número limitado de clientes. Talvez você ainda não consiga acessar essa experiência.

Você pode usar o nível AWS gratuito para explorar AWS serviços sem compromissos de custo. Se você for novo AWS, receberá USD \$100 em créditos depois de criar uma conta, independentemente

do plano da sua conta. Você também pode receber até USD 100 adicionais em créditos para usar em todos os seus projetos ao concluir atividades. Para ter mais informações sobre como conseguir créditos adicionais, consulte [Ganhe créditos adicionais](#). Além disso, você tem acesso a mais de 30 AWS serviços sempre gratuitos que oferecem limites mensais de uso gratuito.

O plano de conta gratuita é ideal para clientes que estão experimentando AWS serviços e criando provas de conceitos sem nenhum custo por até seis meses. Você não será cobrado durante esse período até fazer a atualização para um plano de conta paga. Seu plano de conta gratuita termina após seis meses ou quando seus créditos forem usados totalmente, o que ocorrer primeiro. Além disso, os planos de conta gratuita não têm acesso a determinados AWS serviços que consumiriam rapidamente todo o valor do crédito do nível AWS gratuito ou as compras de hardware. Para obter uma lista dos serviços elegíveis no plano de conta gratuita, consulte [AWS Serviços suportados para Inscrever-se em AWS \(novo\)](#).

O Plano de conta paga é ideal para criar pedidos de produção que superem o valor inicial do crédito. Quando seu uso excede seu saldo de crédito ou quando você usa um serviço em que os créditos não se aplicam, você paga o preço padrão conforme o uso.

Todos os projetos que você possui estão sob o mesmo tipo de plano. Se você fizer o upgrade para o plano de conta paga, todos os seus projetos terão acesso a serviços adicionais e você pagará o preço padrão conforme o uso para todos os projetos. Para obter mais informações, consulte [Atualizar sua conta em AWS Configurações](#).

Você pode usar o Console de gerenciamento de custos para monitorar seu uso em todos os AWS serviços que oferecem o nível gratuito para seu projeto.

Acompanhar seu uso do nível gratuito

Warning

No momento, estamos lançando nossa nova experiência para um número limitado de clientes. Talvez você ainda não consiga acessar essa experiência.

AWS Os alertas de uso do nível gratuito notificam você automaticamente por e-mail quando você excede 85% do limite do nível gratuito para cada serviço. Para um rastreamento adicional, você pode configurar para monitorar seu uso até 100% do limite do nível gratuito definindo um orçamento de gasto zero. Você também pode filtrar seu orçamento para rastrear serviços individuais.

Você pode monitorar seu uso do nível AWS gratuito das seguintes maneiras.

Utilizar AWS Configurações

Você pode monitorar a data de expiração do seu plano de conta gratuita, o saldo de crédito e os dias restantes nas AWS Configurações. Para obter mais informações, consulte [Visualize e resgate créditos em AWS Configurações](#). Você também recebe alertas periódicos por e-mail sobre o saldo do seu crédito e quando o final do período do seu plano de conta gratuita estiver se aproximando.

Se você tiver um plano pago, poderá monitorar seu saldo de crédito e a data de vencimento na página de créditos em AWS Configurações. Para obter mais informações sobre o upgrade para um plano pago, consulte [Atualize sua conta em AWS Configurações](#).

Usando o console de gerenciamento de cobrança e custos

Você pode usar o console de gerenciamento de cobrança e custos para monitorar o uso do nível gratuito em cada projeto. O console de gerenciamento de cobrança e custos mostra um resumo do seu uso acumulado no mês e de qualquer oferta de serviço igual ou superior aos limites de uso. Para cada oferta de nível gratuito em uso, você pode ver o seguinte:

- O serviço
- O limite de uso do nível AWS gratuito
- Seu uso atual
- Seu uso previsto
- Seu uso real acumulado no mês (MTD)
- Seu uso previsto no acumulado do mês (MTD)

O procedimento a seguir mostra como usar o console de gerenciamento de cobrança e custos para classificar o uso do nível gratuito pelo uso real acumulado no mês.

Para classificar seu uso do nível gratuito

1. Abra o console de Gerenciamento de Faturamento e Custos em <https://console.aws.amazon.com/cost-management/>.
2. Escolha o nível gratuito.
3. Para classificar por uso real acumulado no mês, escolha % de uso real do MTD.

Ganhe créditos adicionais

Warning

No momento, estamos lançando nossa nova experiência para um número limitado de clientes. Talvez você ainda não consiga acessar essa experiência.

Se você for um novo AWS cliente, poderá ganhar USD \$100 adicionais em créditos, independentemente do plano da sua conta, concluindo as atividades. Essas atividades ajudam você a aprender sobre os AWS serviços. Você pode encontrar as atividades no AWS widget Explorar no painel inicial AWS do console. Todas essas atividades incorrerão em taxas de AWS serviço que serão deduzidas de seus créditos de nível AWS gratuito. No entanto, ao concluir cada atividade, você receberá USD 20 em créditos.

Atividades a serem concluídas

- [Execute uma instância usando o Amazon EC2](#)
- [Use um modelo básico no playground Amazon Bedrock](#)
- [Crie um orçamento](#)
- [Crie um aplicativo web usando o Lambda](#)
- [Crie um banco de dados Amazon RDS](#)

Visualize suas informações de cobrança em AWS Configurações

Warning

No momento, estamos lançando nossa nova experiência para um número limitado de clientes. Talvez você ainda não consiga acessar essa experiência.

Você pode usar AWS as Configurações para visualizar suas informações de cobrança. Se você estiver usando o Nível Gratuito, esta página mostra quantos dias do Nível Gratuito você tem e seus AWS créditos. Você também pode ver o custo por projeto. Se você estiver usando o plano pago, poderá ver seu saldo, cobranças atuais e o custo por projeto. Se você estiver usando um limite de gastos, poderá visualizar as informações relacionadas ao seu limite. Você também pode [Gerencie](#)

[sua forma de pagamento em AWS Configurações](#) [Gerencie o registro fiscal em AWS Configurações](#) e.

Quando você usa o Plano Gratuito, todo o uso é coberto pelos seus créditos do Nível AWS Gratuito. Você precisa fazer o upgrade para o plano pago se esgotar seus créditos do nível AWS gratuito ou após 184 dias, o que acontecer primeiro. Para obter mais informações sobre o upgrade para um plano pago, consulte [Atualize sua conta em AWS Configurações](#).

Para ver seu custo por projeto

1. Abra AWS as configurações em <https://settings.aws.com>.
2. No painel de navegação principal, escolha **Faturamento**.
3. Em **Custo por projeto**, você verá suas cobranças mensais e as cobranças previstas para o mês. Você verá todas as cobranças em seus projetos.
4. (Opcional) Para ver um detalhamento das cobranças de um projeto em **Inspecionar custos**, escolha **Exibir**. Você será redirecionado para o console de gerenciamento de AWS cobrança e custos.

Seus dados de faturamento e os dados do Cost Explorer que você vê no console de gerenciamento de AWS cobrança e custos são atualizados pelo menos uma vez por dia. A cadência com que eles são atualizados pode ser diferente. Se você usar um limite de gastos, isso poderá resultar em diferenças nas cobranças estimadas acumuladas no mês nas AWS Configurações e no Console de Gerenciamento de AWS Custos.

Visualize seu histórico de cobrança em AWS Configurações

Warning

No momento, estamos lançando nossa nova experiência para um número limitado de clientes. Talvez você ainda não consiga acessar essa experiência.

Você pode ver seu histórico de cobrança em AWS Configurações. Seu histórico de cobrança só está disponível se você tiver uma forma de pagamento. Se você estiver usando o nível gratuito, não verá seu histórico de cobrança.

Você pode baixar as faturas de cada provedor de serviços com quem você fez transações durante o período de cobrança. Isso inclui informações como tipo de cobrança, data da fatura e total em USD. Se suas faturas forem emitidas em outra moeda, o total na outra moeda também será exibido. As faturas não são divididas em cada projeto.

Para ver seu histórico de cobrança

1. Abra AWS as configurações em <https://settings.aws.com>.
2. No painel de navegação principal, escolha **Faturamento**.
3. Ao lado de **Saldo**, escolha **Exibir histórico de cobrança**. Você será redirecionado para o histórico de cobrança.
4. Para baixar uma fatura, selecione um ID de fatura.

Gerencie sua forma de pagamento em AWS Configurações

Warning

No momento, estamos lançando nossa nova experiência para um número limitado de clientes. Talvez você ainda não consiga acessar essa experiência.

Você pode gerenciar sua forma de pagamento nas AWS Configurações. Sua forma de pagamento é usada para pagar pelo uso de AWS recursos em todos os seus projetos. Você só pode gerenciar sua forma de pagamento se tiver fornecido informações ao criar sua conta ou se tiver atualizado sua conta para o Plano Pago.

Para gerenciar sua forma de pagamento

1. Abra AWS as configurações em <https://settings.aws.com>.
2. No painel de navegação principal, escolha **Faturamento**.
3. Em **Saldo**, você verá suas informações de pagamento. Escolha **Gerenciar**.
4. Em **Forma de pagamento**, escolha **Atualizar**.
5. Insira sua nova forma de pagamento e escolha **Salvar**.

Faça um pagamento em AWS Configurações

Warning

No momento, estamos lançando nossa nova experiência para um número limitado de clientes. Talvez você ainda não consiga acessar essa experiência.

Você pode pagar sua AWS conta nas AWS Configurações. AWS cobra sua forma de pagamento padrão automaticamente no início de cada mês. Se essa cobrança não for processada com êxito, use o console para atualizar seu método de pagamento e efetuar o pagamento.

Antes de efetuar um pagamento, certifique-se de que a forma de pagamento que você deseja que seja cobrada automaticamente no futuro esteja definida como sua forma de pagamento padrão. Se estiver usando um cartão de crédito, confirme se ele não expirou.

Para efetuar um pagamento

1. Abra AWS as configurações em <https://settings.aws.com>.
2. No painel de navegação principal, escolha **Faturamento**.
3. Ao lado de **Saldo**, escolha **Exibir histórico de cobrança**. Você será redirecionado para o histórico de cobrança.
4. Em **Ação**, você verá **Pagar fatura** de qualquer fatura pendente. Se não houver faturas listadas, você não precisará fazer nada.
5. Escolha **Pagar fatura**.
6. Confirme sua escolha e escolha **Pagar**.

Se você tiver dúvidas sobre problemas com cobrança da sua conta bancária ou pagamento de um saldo vencido, crie um caso no [Support Center \(Atendimento ao cliente\)](#).

Altere sua moeda preferida em AWS Configurações

Warning

No momento, estamos lançando nossa nova experiência para um número limitado de clientes. Talvez você ainda não consiga acessar essa experiência.

Você pode alterar sua moeda preferida nas AWS Configurações. Sua moeda preferida só se aplica aos projetos que você possui. Alguns países de cobrança restringem as moedas de pagamento. O emissor do seu cartão pode cobrar uma taxa pelas transições em outras moedas.

Para alterar sua moeda de exibição preferida

1. Abra AWS as configurações em <https://settings.aws.com>.
2. No painel de navegação principal, escolha **Faturamento**.
3. Em **Saldo**, você verá suas informações de pagamento. Escolha **Gerenciar**. Se você não vê um saldo, não pode alterar a moeda.
4. Escolha **Definir moeda**.
5. Em **Moeda de pagamento padrão**, selecione a moeda de pagamento.
6. Escolha **Salvar**.

Gerencie o registro fiscal em AWS Configurações

Warning

No momento, estamos lançando nossa nova experiência para um número limitado de clientes. Talvez você ainda não consiga acessar essa experiência.

Você gerencia seus números de registro fiscal e isenções fiscais nas AWS Configurações. Suas informações fiscais só se aplicam aos projetos que você possui.

Como atualizar e excluir números de registro fiscal

Use as etapas a seguir para atualizar ou excluir um ou mais números de registro fiscal.

Note

Se um país não constar na lista suspensa da página **Configurações fiscais**, a AWS não coleta o registro fiscal desse país no momento.

Para atualizar os números de registro fiscal

1. Abra AWS as configurações em <https://settings.aws.com>.
2. No painel de navegação principal, escolha Faturamento.
3. Em Saldo, você verá suas informações de pagamento. Escolha Gerenciar.
4. Escolha Configurações fiscais.
5. Modifique suas informações de registro fiscal.
6. Escolha Salvar.

Gerenciar suas isenções fiscais nos EUA

Se seu estado for elegível, você poderá gerenciar suas isenções fiscais dos EUA na página Plano e cobrança em Configurações. AWS Os documentos enviados para obter a isenção são analisados pelo Suporte em 24 horas. Você só pode gerenciar suas isenções fiscais se sua conta estiver registrada como uma empresa.

Para carregar ou adicionar sua isenção fiscal dos EUA

1. Abra AWS as configurações em <https://settings.aws.com>.
2. No painel de navegação principal, escolha Faturamento.
3. Em Saldo, você verá suas informações de pagamento. Escolha Gerenciar.
4. Escolha Manage tax exemption (Gerenciar isenção de impostos) e selecione Add tax exemption (Adicionar isenção fiscal).
5. Especifique seu tipo de isenção e jurisdição.
6. Carregue os documentos de certificado.
7. Revise suas informações e escolha Submit (Enviar).

Em 24 horas, o Suporte notificará você por meio de um caso de suporte se precisar de informações adicionais ou se algum dos seus documentos não for válido.

Depois que a isenção for aprovada, você a verá na guia Tax exemption (Isenção de impostos) com um período de validade Ativo.

Você será notificado por meio de um contato de caso de suporte se sua isenção for rejeitada.

Visualize e resgate créditos em AWS Configurações

Warning

No momento, estamos lançando nossa nova experiência para um número limitado de clientes. Talvez você ainda não consiga acessar essa experiência.

Você pode visualizar e resgatar seus créditos disponíveis nas AWS Configurações. AWS os créditos são aplicados automaticamente às contas para ajudar a cobrir os custos associados aos serviços elegíveis. Para obter mais informações sobre serviços qualificados, consulte [Resgatar seu crédito AWS promocional](#). Os créditos são aplicados em todos os projetos que você possui até que eles se esgotem ou expirem. Você não pode selecionar qual projeto usa os créditos que você resgata, eles são aplicados em todos os projetos que você possui.

Para ver seus créditos

1. Abra AWS as configurações em <https://settings.aws.com>.
2. No painel de navegação principal, escolha Faturamento.
3. No contêiner Cobranças atuais, você verá seus créditos disponíveis. Escolha seus créditos.

Você será redirecionado para uma visualização dos créditos ativos e expirados, ou seus créditos e dos últimos 6 meses de créditos inativos, dependendo do tipo de seu plano.

4. Para ver os AWS serviços que podem ser usados com seus créditos, escolha Ver lista de serviços.

Para resgatar seu AWS Créditos promocionais

1. Abra AWS as configurações em <https://settings.aws.com>.
2. No painel de navegação principal, escolha Faturamento.
3. No contêiner Cobranças atuais, você verá seus créditos disponíveis. Escolha seus créditos.

Você será redirecionado para uma visualização dos créditos ativos e expirados, ou seus créditos e dos últimos 6 meses de créditos inativos, dependendo do tipo de seu plano.

4. Escolha Resgatar crédito para resgatar seus créditos.

5. Para obter o código promocional, insira o código promocional conforme ele aparece. Ao resgatar o crédito, você indica que leu e concorda com os Termos e Condições dos Créditos [AWS Promocionais](#).
6. Escolha Resgatar crédito.

Gerencie contas na Índia em AWS Configurações

Warning

No momento, estamos lançando nossa nova experiência para um número limitado de clientes. Talvez você ainda não consiga acessar essa experiência.

Se você se inscrever AWS e escolher a Índia como seu endereço de contato e cobrança, seu contrato de usuário será com a Amazon Web Services India Private Limited (AWS Índia), um AWS vendedor local na Índia. AWS A Índia gerencia seu faturamento e o total da fatura é listado em rúpias indianas (INR) em vez de dólares americanos (USD).

Se sua conta estiver AWS na Índia, siga os procedimentos neste tópico para gerenciar sua conta. Este tópico explica como se inscrever em uma conta AWS na Índia, editar informações sobre AWS sua conta na Índia, gerenciar a verificação de clientes e adicionar ou editar seu Número de Conta Permanente (PAN).

Tópicos

- [Cadastre-se para AWS \(novo\) com AWS Índia](#)
- [Gerenciar suas informações de verificação do cliente](#)

Cadastre-se para AWS (novo) com AWS Índia

AWS A Índia é um vendedor local AWS de na Índia. Se seu endereço de contato e cobrança for na Índia, use o procedimento a seguir para se inscrever.

Para usar Inscreva-se em AWS (novo) com AWS Índia

1. Acesse aws.amazon.com e escolha Criar conta.
2. No banner que explica as diferenças entre Inscrever-se em AWS (novo) e Inscrever-se em AWS (avançado), escolha Inscrever-se em AWS.

3. Escolha um login, como Google GitHub, Apple ou Amazon.
4. Você será direcionado para o login do seu provedor. Depois de fazer o login, você será redirecionado para se AWS inscrever.
5. Digite seu nome e escolha Continuar.

Esse nome será compartilhado com os membros da equipe quando você der acesso aos seus projetos.

6. Verifique o e-mail associado ao seu login inserindo um código de verificação. Depois de verificar seu e-mail, escolha Continuar.
7. Insira uma senha forte para sua conta e escolha Continuar.

AWS exige que sua senha atenda às seguintes condições:

- Ter no mínimo 8 caracteres e no máximo 128 caracteres de extensão.
 - Deve incluir no mínimo três dos seguintes tipos de caracteres: maiúsculas, minúsculas, números e ! @ # \$ % ^ _ * () < > [] { } | _ + - = símbolos.
 - Não deve ser idêntico ao seu Conta da AWS nome ou endereço de e-mail.
8. Insira seus dados de contato e escolha Continuar.

Se seu endereço de contato ou cobrança estiver localizado na Índia, em conformidade com os regulamentos da Equipe Indiana de Resposta a Emergências de Computadores (CERT-In), AWS é necessário coletar e validar suas informações de identidade antes de conceder acesso aos serviços. AWS

O nome que você escolher para informações de contato ou faturamento deverá corresponder ao nome que consta do documento que você planeja usar para verificação do cliente. Por exemplo, se você planeja verificar uma conta comercial usando um Certificado de Incorporação social, deve fornecer o nome comercial que consta do documento. Para obter uma lista dos tipos de documentos aceitos, consulte [the section called “Documentos da Índia aceitos para verificação do cliente”](#).

9. Escolha a finalidade principal do registro da sua conta.
10. Escolha o tipo de propriedade que representa melhor o proprietário da conta. Se você escolher uma empresa, organização ou parceria como tipo de propriedade, insira o nome de um dos principais membros da administração. Essa pessoa pode ser um diretor, um chefe de operações ou uma pessoa responsável pelas operações da empresa.

11. Dependendo do tipo de propriedade selecionado, escolha um tipo de documento aceito na Índia para usar na verificação e insira as informações do documento.

 Note

Se você tem uma conta pessoal e planeja usar uma carteira de habilitação que não seja emitida pela União da Índia, é recomendável usar um tipo de documento pessoal diferente para verificação.

12. Escolha o nome que você deseja usar para verificação do cliente.

Os nomes das suas informações de faturamento e contato serão exibidos para seleção se estiverem associados a um endereço indiano. Certifique-se de que o nome que você escolher corresponda ao nome que consta do tipo de documento que você planeja usar para a verificação do cliente. Se você precisar fazer alterações no nome associado ao endereço de faturamento ou contato, poderá fazer isso depois de concluir o cadastramento na conta.

13. Forneça seu consentimento para enviar as informações para verificação e escolha Continuar.

Você receberá uma notificação sobre o resultado da verificação do cliente por e-mail depois de concluir o cadastro na conta. Você também pode verificar o status na página do perfil em Minhas AWS configurações. Você deve passar na verificação do cliente para acessar os serviços da AWS .

14. AWS provisionará seu primeiro projeto.

Para acessar AWS as Configurações, escolha Gerenciar projetos no Console de gerenciamento da AWS. Em AWS Configurações, você pode convidar membros da equipe, criar novos projetos e modificar seu faturamento e outras configurações.

Gerenciar suas informações de verificação do cliente

Em conformidade com os regulamentos da Equipe Indiana de Resposta a Emergências de Computadores (CERT-In), AWS é necessário coletar e validar suas informações de identidade antes de conceder a você acesso novo ou contínuo aos AWS serviços. Sua identidade deve ser verificada usando o nome fornecido por você no endereço de faturamento ou de contato na Índia. Durante a verificação, AWS verificará se o número do documento é válido e se o nome fornecido corresponde ao nome associado ao documento usado para verificação do cliente. O nome que você escolher para

informações de contato ou faturamento deverá corresponder exatamente ao nome que consta do documento.

Para atualizar seu nome de cobrança, endereço e outras informações de contato, consulte [Use AWS Configurações](#). Se você editar qualquer informação usada anteriormente para verificação do cliente, como nome ou India-based endereço das informações de contato ou cobrança, talvez seja necessário atualizar e reenviar as informações de verificação do cliente.

Verificar o status da sua verificação do cliente

Você pode ver o status de verificação do cliente a qualquer momento na página Gerenciar perfil. Se o status da sua verificação for Verificação necessária ou Falha na verificação, crie ou atualize suas informações de verificação do cliente e envie-as novamente para verificação.

Criar suas informações de verificação do cliente

Para concluir a verificação do cliente, você precisará fornecer informações de um documento aceito na Índia. Para obter uma lista dos tipos de documentos aceitos, consulte [the section called “Documentos da Índia aceitos para verificação do cliente”](#).

1. Abra AWS as Configurações em <https://settings.aws.com>.
2. No painel de navegação principal, escolha Gerenciar perfil.
3. Em Verificação do cliente, escolha Criar verificação do cliente.
4. Escolha um nome que corresponda exatamente ao nome que consta do documento que você planeja usar para a verificação do cliente. Por exemplo, se você planeja verificar uma conta comercial usando um Certificado de Incorporação social, deve fornecer o nome comercial que consta do documento.
5. Forneça as informações remanescentes solicitadas na página. Dependendo do tipo de documento escolhido, talvez seja necessário carregar uma cópia da frente e do verso do documento. Se você carregar um arquivo de imagem, verifique se todas as informações constantes do documento estão visíveis e legíveis.
6. Selecione Enviar.

Você será notificado sobre o resultado da verificação do cliente e sobre as próximas etapas por e-mail ou no AWS Health Dashboard.

Editar suas informações de verificação do cliente

Você pode editar suas informações de verificação do cliente, como o objetivo principal do registro da conta, o tipo de organização e o nome, o tipo de documento, o carregamento do documento ou as informações do documento que você deseja usar para verificação.

Se você editar o nome ou o tipo de documento a ser usado na verificação do cliente ou se atualizar quaisquer informações do documento, para salvar as alterações será necessário verificar sua identidade novamente.

1. Abra AWS as Configurações em <https://settings.aws.com>.
2. No painel de navegação principal, escolha Gerenciar perfil.
3. Em Verificação do cliente, escolha Verificação do cliente.
4. Escolha Editar e, em seguida, atualize as informações que você deseja alterar.

Ao atualizar as informações, observe as seguintes orientações:

- Se você escolher um nome diferente, o nome deverá corresponder exatamente ao nome que consta do documento que você planeja usar para a verificação do cliente. Por exemplo, se você planeja verificar uma conta comercial usando um Certificado de Incorporação social, deve fornecer o nome comercial que consta do documento.
 - Se você escolher um tipo de documento diferente, precisará carregar uma cópia da frente e do verso (se aplicável) do documento. Todas as informações no carregamento do documento devem estar visíveis e legíveis.
 - Se você tem uma conta pessoal e planeja usar uma carteira de habilitação que não seja emitida pela União da Índia, é recomendável usar um tipo de documento pessoal diferente para verificação.
 - Para obter uma lista dos tipos de documentos aceitos, consulte [the section called “Documentos da Índia aceitos para verificação do cliente”](#).
5. Selecione Enviar.

Se sua identidade precisar ser verificada novamente devido ao tipo de alteração que você salvou, você receberá uma notificação do resultado da verificação do cliente e das próximas etapas por e-mail. Você também pode ver os resultados retornando à página de verificação do cliente ou ao AWS Health Dashboard.

Documentos da Índia aceitos para verificação do cliente

Os seguintes tipos de documentos emitidos pelo governo indiano são aceitos para verificação do cliente.

Note

Os links compartilhados abaixo estão sujeitos a alterações pelo governo.

- **Cartão de PAN:** disponível em formato digital e físico, o cartão de número de conta permanente (PAN) contém um identificador alfanumérico exclusivo emitido pelo Income Tax Department of India para indivíduos, empresas e entidades. Um PAN consiste em dez caracteres, incluindo letras e números, no formato **AAAAA1111A**. Para usar esse documento para verificação, você também deve fornecer a data de nascimento (pessoa física) ou a data de incorporação (empresa) exibida no cartão de PAN e carregar a frente do cartão. Consulte o [site oficial do Income Tax Department](#) para verificar a validade do PAN.
- **Identificação do eleitor Card/EPIC** - A carteira de eleitor, também conhecida como Carteira de Identidade com Foto do Eleitor (EPIC), contém um número de identificação exclusivo emitido pela Comissão Eleitoral da Índia para eleitores elegíveis na Índia. O ID/EPIC número do eleitor consiste em dez caracteres, incluindo letras e números. Acesse o site oficial da [Election Commission of India](#) para verificar a validade do seu título de eleitor. Para usar esse documento para verificação, você deve carregar a frente e o verso do cartão.
- **Carteira de habilitação:** se sua carteira de habilitação não for emitida pela União da Índia, recomendamos o uso de um tipo de documento diferente para verificação. O número da carteira de habilitação consiste em 12 a 16 caracteres, incluindo letras, números e um espaço ou hífen. Para usar esse documento para verificação, você deve informar sua data de nascimento e carregar a frente e o verso do cartão. Acesse o [site Parivahan Sewa](#) do Ministry of Road Transport and Highways para verificar a validade da sua carteira de habilitação.
- **Certificado de Incorporação:** um certificado de incorporação é um documento emitido pelo Ministry of Corporate Affairs (MCA), que data o registro de uma empresa como pessoa jurídica. O certificado é usado para identificar e rastrear de forma exclusiva empresas registradas na Índia. Cada certificado contém um Número de Identificação Corporativa (CIN), que é um identificador alfanumérico exclusivo que consiste em 21 caracteres, incluindo letras e números. Para usar esse documento para verificação, você deve carregar o documento do certificado de incorporação. Você pode acessar o [portal do Ministry of Corporate Affairs](#) para verificar a validade do CIN.

Diferentes tipos de documentos da Índia são aceitos para contas pessoais e comerciais:

- Para contas pessoais - cartão PAN, carteira de eleitor e carteira de habilitação. card/EPIC
- Para contas comerciais: cartão de PAN e certificado de incorporação.

Configure seu faturamento na Índia em AWS Configurações

Warning

No momento, estamos lançando nossa nova experiência para um número limitado de clientes. Talvez você ainda não consiga acessar essa experiência.

Se você se inscrever AWS e escolher a Índia como seu endereço de contato e cobrança, seu contrato de usuário é com a Amazon Web Services India Private Limited (AWS Índia), um AWS vendedor local na Índia. AWS A Índia gerencia seu faturamento e o total da fatura é listado em rúpias em vez de dólares. Todas as informações fiscais só podem ser criadas ou modificadas pelo proprietário do projeto.

Para obter informações adicionais sobre impostos ou cobrança, você pode usar o AWS Billing console para cada projeto.

Use a seção Plano e cobrança na página Gerenciar perfil das AWS Configurações para realizar as seguintes tarefas:

- Adicionar ou editar um número de conta permanente
- Editar vários números de conta permanente
- Editar vários números de impostos sobre bens e serviços
- Visualizar uma fatura fiscal

Adicionar ou editar um número de conta permanente (PAN)

É possível adicionar seu número de conta permanente (PAN) à sua conta e editá-lo.

Adicionar ou editar um PAN

1. Abra AWS as configurações em <https://settings.aws.com>.

2. No painel de navegação principal, escolha Gerenciar perfil e, em seguida, escolha Plano e cobrança.
3. Na barra de navegação Tax Settings, escolha Edit.
4. Em Permanent Account Number (PAN), digite o PAN e escolha Update.

Editar vários números de conta permanente

Você pode editar vários números de conta permanente (PANs) na sua conta.

Para editar vários números de PAN

1. Abra AWS as configurações em <https://settings.aws.com>.
2. No painel de navegação principal, escolha Gerenciar perfil e, em seguida, escolha Plano e cobrança.
3. Em Manage Tax Registration Numbers (Gerenciar números de registro fiscal), selecione os números de PAN que você deseja editar.
4. Em Manage Tax Registration (Gerenciar registro fiscal), escolha Edit (Editar).
5. Atualize os campos que você deseja alterar e escolha Update (Atualizar).

Editar vários números de impostos sobre bens e serviços

Você pode editar vários números de GST (Imposto sobre bens e serviços) na sua conta.

Para editar vários números de GST

1. Abra AWS as configurações em <https://settings.aws.com>.
2. No painel de navegação principal, escolha Gerenciar perfil e, em seguida, escolha Plano e cobrança.
3. Em Manage Tax Registration Numbers (Gerenciar números de registro fiscal), selecione os números de GST que você deseja editar ou escolha Edit all (Editar todos).
4. Em Manage Tax Registration (Gerenciar registro fiscal), escolha Edit (Editar).
5. Atualize os campos que você deseja alterar e escolha Update (Atualizar).

Visualizar uma fatura fiscal

Você pode ver suas faturas fiscais em AWS Configurações.

Visualizar uma fatura fiscal

1. Abra AWS as configurações em <https://settings.aws.com>.
2. No painel de navegação principal, escolha Gerenciar perfil e, em seguida, escolha Plano e cobrança.
3. Role para baixo e escolha a aba Invoices (Faturas).
4. Na seção Notas fiscais, escolha um link de fatura mencionado em ID do documento.

Note

A seção Tax invoices (Faturas fiscais) só aparecerá se houver faturas fiscais disponíveis.

Alterando o vendedor do registro de ou para AWS Índia

Você pode alterar seu Conta da AWS vendedor registrado (SOR) para outro SOR atualizando suas informações fiscais ou de cobrança. Isso não se aplica se sua conta AWS na Índia estiver operando no modelo antigo em que a funcionalidade não está disponível. Quando você edita seu país ou região em seus detalhes fiscais ou de cobrança da , o SOR da sua conta mudará automaticamente se o provedor de serviços do novo local for diferente de seu local atual.

Se você estiver alterando sua conta de ou para a AWS Índia, não precisará atualizar sua forma de pagamento padrão se ela estiver definida como fatura ou transferência bancária. Se sua forma de pagamento padrão for cartão de crédito ou débito, você precisará reconfirmar os detalhes do cartão de pagamento padrão. Essa ação garante que a forma de pagamento seja armazenada separadamente das transações que ocorrerem fora da AWS Índia. Para obter mais informações, consulte [Visualização de cartões de crédito ou débito qualificados para faturas AWS](#) da Índia.

Note

Se você tiver uma conta AWS na Índia com um cartão de crédito ou débito como forma de pagamento padrão e tiver um mandato eletrônico configurado para pagamentos automáticos,

deverá desativar o mandato eletrônico antes de editar suas preferências de pagamento padrão.

Para alterar o SOR da sua conta, você pode editar essas informações usando as seguintes opções:

Para alterar o SOR usando informações de cobrança e impostos

1. Abra AWS as configurações em <https://settings.aws.com>.
2. No painel de navegação principal, escolha Gerenciar perfil e, em seguida, escolha Plano e cobrança.
3. Na seção Default payment preferences (Preferências de pagamento padrão), escolha Edit (Editar).
4. Digite o novo endereço de cobrança.
5. Na seção Moeda de pagamento, selecione uma moeda padrão na lista de moedas aceitas do seu novo SOR.
6. Se sua forma de pagamento padrão for cartão de crédito ou débito: na seção Confirmar forma de pagamento, insira novamente os detalhes do seu cartão de pagamento padrão para confirmar o uso com o novo provedor de serviços.

Para alterar os cartões definidos como padrão para o novo SOR, adicione seu cartão posteriormente e altere a configuração da forma de pagamento padrão.

7. Escolha Salvar alterações.

Depois de alguns minutos, suas alterações, incluindo o SOR atualizado, aparecem na página Preferências de pagamento.

Para alterar o SOR usando informações de cobrança e impostos

Para mover sua conta para um SOR diferente, você deve atualizar o número de registro fiscal (TRN) associado à conta e fornecer um novo TRN válido. Você também pode excluir o TRN associado à conta. O novo SOR da sua conta é resolvido automaticamente com base no país do seu novo endereço fiscal e no seu endereço de cobrança atual, em ordem de disponibilidade e prioridade. Quando o SOR da sua conta mudar, você receberá uma notificação de que sua conta está entrando ou saindo da AWS Índia.

1. Abra AWS as configurações em <https://settings.aws.com>.

2. No painel de navegação principal, escolha Gerenciar perfil e, em seguida, escolha Plano e cobrança.
3. Selecione sua conta e depois Gerenciar registro fiscal. Em seguida, selecione Editar, Editar tudo ou Excluir TRN.
4. (Se sua forma de pagamento padrão for cartão de crédito ou débito) No painel de navegação principal, escolha Gerenciar perfil e, em seguida, escolha Plano e cobrança.
5. Selecione Adicionar forma de pagamento para inserir novamente os dados do seu cartão de pagamento padrão ou adicionar um novo cartão de pagamento.
6. Depois de salvar o cartão, selecione Definir como padrão.

A seção Preferências de pagamento padrão alerta que sua forma de pagamento padrão anterior não é aceita para uso no novo SOR. Atualize a página depois de adicionar seu cartão de pagamento para que esse alerta desapareça.

Acesso AWS Suporte

Warning

No momento, estamos lançando nossa nova experiência para um número limitado de clientes. Talvez você ainda não consiga acessar essa experiência.

Quando você se inscreve em nossa nova AWS experiência, há dois lugares onde você pode trabalhar com o AWS Support.

Você pode acessar o Basic Support ou o Business Support+. Por padrão, você está inscrito no Basic Support. Você pode iniciar um teste do Business Support+ para usá-lo gratuitamente por até seis meses.

Apoio ao projeto

Se você estiver enfrentando problemas com seu projeto, com o gerenciamento de sua equipe ou com problemas relacionados ao faturamento, acesse Basic Support ou Business Support+ em Configurações. AWS Você pode solicitar projetos adicionais para sua organização ou solicitar aumentos de cota relacionados ao faturamento.

Como criar um caso de suporte

1. Abra AWS as Configurações em <https://settings.aws.com>.
2. No painel de navegação principal, escolha Support.
3. Para suporte do Project, escolha Criar caso.
4. Em Assunto, insira o assunto do seu caso de suporte.
5. Em Descrição, descreva seu problema. Se possível, descreva as etapas para reproduzir o problema.
6. Escolha Criar caso.

Depois de criar um caso de suporte, você pode ver as informações do seu caso para continuar trabalhando com o suporte.

Para ver as informações do seu caso

1. Abra AWS as Configurações em <https://settings.aws.com>.
2. No painel de navegação principal, escolha Support.
3. Escolha seu caso de suporte. Nessa visualização, você pode ver todas as comunicações sobre o seu caso.
4. Para enviar uma resposta ao suporte, em Responder, insira sua resposta e escolha Enviar resposta.

Quando seu caso for resolvido, você poderá resolvê-lo para removê-lo das AWS Configurações.

Para resolver seu caso

1. Abra AWS as Configurações em <https://settings.aws.com>.
2. No painel de navegação principal, escolha Support.
3. Escolha Resolve case (Resolver caso).

Você não poderá acessar os detalhes do caso depois que ele for resolvido.

Technical support (Suporte técnico)

Se você estiver tendo problemas com seus AWS recursos, precisará de suporte técnico. Para acessar o suporte técnico, abra um caso no [AWS Support Center](#) para o projeto que tem o problema.

Support se todos os seus projetos e organização estiverem fechados

Se todos os seus projetos e sua organização estiverem fechados, entre em contato com o suporte preenchendo o [formulário Support Feedback](#).

Na seção Solicitar informações, em Como podemos ajudá-lo, inclua que você está usando nossa nova AWS experiência e que todos os seus projetos estão encerrados.

Inicie um teste do Business Support+

Você pode obter o Business Support+ gratuitamente por até seis meses. O Business Support+ é fornecido gratuitamente até 31 de outubro de 2026. A partir de 1º de novembro de 2026, o preço padrão começa e você receberá \$174 em créditos Business Support+ para cobrir até seis meses de USD \$29 por mês. Você permanece inscrito quando o período gratuito termina e os créditos começam, e AWS notifica quando seu saldo de crédito está acabando antes que qualquer cobrança de preço total comece.

Sua cobrança do Business Support+ é \$ 29/month ou uma porcentagem de seus AWS gastos, o que for maior. Para obter mais informações, consulte os [detalhes de preços](#). Seu plano é renovado mensalmente até você cancelar.

Para iniciar seu teste do Business Support+

1. Abra AWS as Configurações em <https://settings.aws.com>.
2. No painel de navegação principal, escolha Support.
3. Escolha Iniciar teste. Isso afetará todos os projetos em sua organização.
4. Revise os termos, marque a caixa de seleção do contrato e escolha Iniciar teste.

Você pode cancelar a qualquer momento, sem compromisso e sem penalidade. Quando você cancela, o acesso ao Business Support+ termina imediatamente e todos os créditos não utilizados são perdidos. Você pode se inscrever novamente pelo preço padrão a qualquer momento, mas a oferta promocional Business Support+ não pode ser restabelecida depois de cancelada.

Para cancelar o Business Support+

1. Abra AWS as Configurações em <https://settings.aws.com>.
2. No painel de navegação principal, escolha Support.
3. Escolha Cancelar plano.

4. Marque a caixa de seleção para confirmar que o cancelamento do Business Support+ retornará você ao Suporte Básico imediatamente, que você perderá o acesso aos benefícios listados e que seus \$174 em créditos serão removidos e não poderão ser restabelecidos.
5. Escolha Cancelar plano para retornar ao Basic Support.

Monitore seu projeto usando AWS CloudTrail

Warning

No momento, estamos lançando nossa nova experiência para um número limitado de clientes. Talvez você ainda não consiga acessar essa experiência.

Monitore seu projeto usando AWS CloudTrail

Seu projeto é integrado com AWS CloudTrail, um serviço que fornece um registro das ações realizadas por um membro da equipe ou AWS serviço. CloudTrail captura todas as chamadas de API do seu projeto como eventos. As chamadas capturadas incluem chamadas do console e operações de API para todos os AWS serviços compatíveis. Usando as informações coletadas por CloudTrail, você pode determinar a solicitação que foi feita ao seu projeto, a pessoa que fez a solicitação, quando ela foi feita e detalhes adicionais.

Use CloudTrail para ver quem modificou seu projeto

Este tutorial é para usuários que se sentem confortáveis com AWS CLI o. Se você compartilhar seu projeto com vários membros da equipe, poderá usá-lo CloudTrail para ver quem modificou quaisquer recursos em seu projeto. Todas as ações tomadas por você ou pelos membros da equipe quando eles usam AWS as Configurações ou o Console de gerenciamento da AWS para acessar seu projeto são registradas pelo `onBehalfOf` parâmetro. Esse parâmetro mostra uma ID de usuário e uma ID do repositório de identidades. Juntos, esses valores definem um ID de construtor que você convidou para acessar seu projeto.

Para encontrar o `onBehalfOf` parâmetro e conectá-lo a um membro da equipe, você precisará acessar o AWS CLI e Console de gerenciamento da AWS o. Se você não tiver o AWS CLI configurado, poderá usá-lo AWS CloudShell para acessar um shell pré-autenticado baseado em navegador que você pode iniciar diretamente dos Console de gerenciamento da AWS comandos e executá-los. AWS CLI

Etapa 1. Para encontrar um AWS CloudTrail Evento

1. Faça login no Console de gerenciamento da AWS e abra o CloudTrail console em <https://console.aws.amazon.com/cloudtrail/>.
2. No painel de navegação, escolha Event history (Histórico de eventos). Você verá uma lista filtrada de eventos, com os eventos mais recentes exibidos primeiro. Escolha um evento.
3. No registro do evento, você verá o seguinte conteúdo:

```
"onBehalfOf": {  
    "userId": "00000-e00f-000-000-00000000",  
    "identityStoreArn":  
    "arn:aws:identitystore::111122223333:identitystore/000000-0000-0000-0000-600000007"  
}
```

Essa é a identidade que define o membro da equipe que criou o CloudTrail evento.

Etapa 2. Para conectar o BehalfOf parâmetro on a um membro da equipe

Para conectar o onBehalfOf parâmetro a um membro da equipe usando AWS CLI:

Para usar o AWS CLI no seu terminal

1. Execute o comando a seguir para entrar no AWS CLI. Você pode encontrar sua região usando [Regiões da AWS para seus projetos](#).

```
aws login --region project-region
```

2. Execute o comando a seguir para obter o ID do seu repositório de identidades. O CloudTrail evento mostra o ARN do repositório de identidades, mas não indica o ID do repositório de identidades. Você sempre usa o Região da AWS us-east-1 ao encontrar o ID do seu repositório de identidades.

```
aws sso-admin list-instances --region us-east-1
```

A saída será exibida da seguinte forma:

```
{  
    "Instances": [  
        {
```

```

    "InstanceArn": "arn:aws:sso:::instance/ssoins-00000000000",
    "IdentityStoreId": "d-000000",
    "OwnerAccountId": "111122223333",
    "CreateDate": "2025-10-26T23:10:58.529000+00:00",
    "Status": "ACTIVE",
    "PrimaryRegion": "us-east-1",
    "Regions": [
      {
        "RegionName": "us-east-1",
        "Status": "ACTIVE",
        "AddedDate": "2025-10-26T23:10:58.529000+00:00",
        "IsPrimaryRegion": true
      }
    ]
  }
}

```

Você deseja copiar o ID do repositório de identidades. Nesse caso, o ID do repositório de identidades é `d-000000`.

3. Execute o comando a seguir para descrever o membro da equipe que corresponde ao `onBehalfOf` parâmetro.

```
aws identitystore describe-user --user-id 00000-e00f-000-000-00000000 --region us-east-1 --identity-store-id d-000000
```

A saída será exibida da seguinte forma:

```

{
  "IdentityStoreId": "d-000000",
  "UserId": "00000-e00f-000-000-00000000",
  "UserName": "carlos_salazar",
  "Name": {
    "FamilyName": "Salazar",
    "GivenName": "Carlos"
  },
  "DisplayName": "Carlos",
  "Emails": [
    {
      "Value": "carlos_salazar@example.com",
      "Type": "work",

```

```
        "Primary": true
      }
    ],
    "UserStatus": "ENABLED",
    "CreatedAt": "2025-10-26T23:15:27.213000+00:00",
    "CreatedBy": "000000000000",
    "UpdatedAt": "2025-10-26T23:18:55.432000+00:00",
    "UpdatedBy": "000000000000"
  }
```

O nome de exibição e os e-mails do membro da sua equipe são fornecidos nesta saída.

Para conectar o `onBehalfOf` parâmetro a um membro da equipe usando AWS CloudShell, faça login no Console de gerenciamento da AWS e acesse CloudShell. Para obter mais informações, consulte [Introdução ao AWS CloudShell](#). Você terá automaticamente as permissões corretas do IAM para acessar CloudShell.

Fechar um projeto em AWS Configurações

Warning

No momento, estamos lançando nossa nova experiência para um número limitado de clientes. Talvez você ainda não consiga acessar essa experiência.

Se você não precisar mais do seu projeto, você pode fechá-lo. Depois de fechar seu projeto, você poderá reabri-lo em até 90 dias a partir do dia em que você o fechou. O tempo entre o dia em que você fechou o projeto e o encerramento AWS permanente do projeto é o período pós-encerramento.

O que você precisa saber antes de fechar seu projeto

Antes de fechar seu projeto, considere o seguinte:

- Você não pode fechar seu projeto se ele estiver pausado por exceder um limite de gastos. Você precisa desativar os limites de gastos e depois fechar o projeto. Para obter mais informações, consulte [Atualizar um limite de gastos em AWS Configurações](#).
- Todos os membros da equipe perderão automaticamente o acesso a esse projeto e a todos os recursos dentro dele.

- O encerramento do seu projeto servirá como sua notificação de rescisão do Contrato AWS do Cliente para este projeto.
- Você não precisa excluir recursos do seu projeto antes de fechá-lo. No entanto, recomendamos que você faça backup de todos os recursos ou dados que deseja manter. Para obter instruções sobre como fazer backup de um recurso específico, consulte a AWS documentação apropriada para esse serviço.
- Você pode reabrir seu projeto durante o período pós-encerramento. As cobranças pelos serviços que permaneceram em seu projeto serão reiniciadas se você o reabrir. Você também permanece responsável por quaisquer faturas não pagas.
- Você permanece responsável por todas as taxas e encargos pendentes pelos serviços consumidos antes do encerramento do projeto. Você receberá uma AWS fatura no mês seguinte após o encerramento do projeto. Por exemplo, se você tiver fechado a conta em 15 de janeiro, receberá uma fatura no início de fevereiro pelo uso incorrido de 1.º de janeiro a 15 de janeiro.
- Depois que um projeto for encerrado, AWS enviaremos e-mails diários por até cinco dias antes de suspendermos o domínio. Depois que o domínio for suspenso e dependendo do registrador do domínio, excluiríamos o domínio em 30 dias ou liberaremos o domínio para o registrador. Para obter mais informações, consulte [Meu Conta da AWS está fechado ou permanentemente fechado e meu domínio está registrado no Route 53](#). Essas informações foram escritas para Contas da AWS, mas são precisas para projetos.
- AWS CloudTrail é um serviço de segurança fundamental. Isso significa que as trilhas criadas pelos usuários podem continuar existindo e entregar eventos mesmo após o fechamento de um projeto, a menos que um usuário exclua explicitamente as trilhas em seu projeto antes de fechá-lo. Para obter mais informações sobre como solicitar a exclusão de trilhas após o fechamento de uma Conta da AWS, consulte [Conta da AWS encerramento e trilhas](#) no Guia do CloudTrail usuário. Essas informações foram escritas para Contas da AWS, mas as informações são precisas para projetos.

Para fechar um projeto

Para fechar um projeto

1. Abra AWS as configurações em <https://settings.aws.com>.
2. No painel de navegação principal, escolha o projeto que você deseja acessar.
3. Em Fechar projeto, escolha Fechar projeto.
4. Confirme sua escolha e escolha Fechar projeto.

A página do projeto ainda mostrará seu projeto por 90 dias até que ele seja excluído permanentemente.

Post-closure período

O período pós-encerramento se refere ao período de tempo entre o dia em que você fechou sua conta e o encerramento AWS permanente do projeto. O período pós-encerramento é de 90 dias. Durante o período pós-encerramento, você pode acessar seu conteúdo e AWS serviços somente reabrindo seu projeto. Após o período pós-encerramento, fecha AWS permanentemente seu projeto e você não poderá mais reabri-lo. AWS também excluirá conteúdo e recursos da sua conta (exceto CloudTrail trilhas). Depois que um projeto é fechado permanentemente, seu ID de projeto nunca pode ser reutilizado.

Reabrindo seu projeto

Seu projeto será encerrado permanentemente em 90 dias, após os quais você não poderá reabri-lo e AWS excluirá o conteúdo restante em seu projeto. Para reabrir seu projeto antes que ele seja encerrado permanentemente, (1) você deve entrar em contato o mais rápido Suporte possível e (2) devemos receber o pagamento integral de qualquer saldo pendente, incluindo o fornecimento das informações necessárias conforme especificado na fatura, dentro de 60 dias a partir da data de encerramento da conta.

Note

As cobranças pelos serviços que permaneceram em seu projeto serão reiniciadas se você o reabrir.

Ativar avançado AWS recursos

Warning

No momento, estamos lançando nossa nova experiência para um número limitado de clientes. Talvez você ainda não consiga acessar essa experiência.

Ao ativar os recursos avançados, você assume o controle total da AWS organização, da conta de gerenciamento e da conta de administrador delegado que são usadas para gerenciar os projetos que

you created and the team members that you invited. You will manage security, governance, and participation in the team of your AWS environment. You have access to AWS services, additional resources, multi-region resources, and administrative and billing controls.

You must update your account before you activate advanced resources. For more information, consult [Update your account in AWS Configurations](#).

What happens when you activate advanced resources

When you activate advanced resources, the following changes will be applied immediately to your account and to the AWS organization that contains your projects:

- Now you are the administrator of the AWS organization that contains your projects.
- You define a root email address for your account. You will also need to define a root user password. For more information, consult [Define a password for the root user for your account](#).
- You manage your projects as member accounts in your organization. As administrator of this organization, you can create member accounts in the organization. Your AWS Builder ID continues to be the owner of your project accounts. For more information, consult [Project accounts after activating advanced resources](#).
- To assign an administrator role to member accounts that you invite to join your organization, you must create an `OrganizationAccountAccessRole`. For more information, consult [Creation of OrganizationAccountAccessRole in a member account](#).
- The members of your team are called identities in the workforce and can still access their AWS accounts. You can also choose to customize the source of identity for your workforce using the IAM Identity Center. You can continue using the AWS Builder ID as the source of identity or change it to an external source of identity. If you change the source of identity from the AWS Builder ID to another source of identity, this change is irreversible. You cannot reactivate the AWS Builder ID as the source of identity in the future. For more information, consult [Change source of identity of AWS ID of the builder](#).
- You control AWS access for users and groups in the organization using the IAM Identity Center using the Account Access Manager. You can use this resource to modify access for the user and, at the same time, allow your users to log in using `aws login` to receive their session credentials from the IAM of the browser. For more information, consult [Access manager to AWS account](#).

- AWS cria uma conta de membro chamada Identity Delegated Admin em sua organização com uma função de administrador delegado. Essa função é usada para realizar a maioria das tarefas administrativas no IAM Identity Center e no gerente de acesso à conta. A função de administrador delegado deve ser usada no Leste dos EUA (Norte da Virgínia). Para ter mais informações, consulte [Delegated administration](#).

Seu ID do AWS Builder possui a conta Identity Delegated Admin, assim como suas contas de projeto.

- Agora você pode configurar Políticas de Controle de Recursos (RCPs) e Políticas de Controle de Serviços (SCPs) para impor proteções personalizadas em sua organização. Anteriormente, AWS gerenciava RCPs e SCPs em seu nome. Você pode modificar essas políticas depois de ativar os recursos avançados. Para obter mais informações, consulte [Remover políticas da organização](#).

Quando você ativa os recursos avançados, as seguintes alterações também são aplicadas à sua AWS organização:

- Se você tiver um limite de gastos para qualquer uma das suas AWS contas, ele será removido. Todos os projetos atualmente pausados serão reativados. Você não pode criar um limite de gastos se ativar recursos avançados. Em vez disso, você tem acesso a todo o conjunto de ferramentas de Billing and Cost Management. Isso inclui definir orçamentos, baixar relatórios do Cost Explorer e detectar gastos incomuns com o AWS Cost Anomaly Detection. Você pode usar essas ferramentas avançadas para analisar, organizar, planejar e otimizar seus custos.
- Você pode acessar todos os AWS serviços. Os serviços disponíveis estão listados em [the section called “Serviços da AWS não é compatível com nosso novo AWS experiência”](#). Você deve planejar sua arquitetura e consultar a documentação do serviço antes de habilitar esses serviços. Além disso, o Agent Toolkit fornece muitas [habilidades](#) para trabalhar com esses serviços.
- Você obtém acesso a regiões adicionais Regiões da AWS opcionais e acesso a recursos multirregionais. Multi-Region a arquitetura melhora a resiliência de suas cargas de trabalho. Recomendamos que você planeje como restringirá e auditará sua presença regional. É importante garantir que os recursos que você cria estejam presentes somente nas regiões que você pretende usar.
- Você pode desativar o gerenciador de funções do IAM para cada um Conta da AWS em sua organização. O gerenciador de funções do IAM é uma configuração de conta opcional que provisiona automaticamente as funções, para que você e sua força de trabalho não precisem configurá-las. Para obter mais informações, consulte [Como ativar e desativar o gerenciador de funções \(console\)](#).

- Você pode usar o [IAM Access Analyzer](#).

Quando você ativa recursos avançados, as seguintes alterações também são aplicadas à sua experiência de usuário:

- Anteriormente, Console de gerenciamento da AWS mostrava uma visualização simplificada com um menu que você usava para alternar entre projetos e acessar AWS as Configurações. Isso Console de gerenciamento da AWS se expande para incluir recursos adicionais, como seletor de regiões, serviços adicionais e configuração de uma cor para a conta que você possa acessar para distinguir visivelmente entre elas. Para obter mais informações, consulte [Recursos do console](#).
- Agora você também pode fazer o seguinte:
 - Desative o suporte ao console multissessão.
 - Designe sua AWS conta como compatível com HIPAA ou SEC.
 - Use o AWS Marketplace.
 - Ganhe créditos extras com o AWS Activate.
 - Trabalhe com um parceiro AWS de treinamento.
 - Compre uma assinatura do AWS Skill Builder Team.
 - Inscreva-se em um contrato empresarial com AWS.
 - Crie um contrato de serviços profissionais.
 - Junte-se à AWS Partner Network.

Contas do projeto depois de ativar os recursos avançados

Cada projeto que você criou nas AWS Configurações contém uma Conta da AWS, chamada de conta de projeto. Uma ID do AWS Builder é proprietária de cada conta do projeto em vez do endereço de e-mail do usuário raiz. Quando você ativa recursos avançados, suas contas de projeto se tornam contas de membros em sua organização, e sua ID do AWS Builder continua sendo sua proprietária, mesmo que você altere posteriormente sua fonte de identidade. Seu AWS Builder ID também possui a conta Identity Delegated Admin que é AWS criada quando você ativa recursos avançados.

Como uma conta de projeto não tem um endereço de e-mail de usuário raiz, ela funciona de forma diferente das outras contas de membros em sua organização:

- O endereço de e-mail que o AWS Organizations console mostra para uma conta de projeto é um espaço reservado que é AWS gerado. As `GetPrimaryEmail`, `DescribeAccount`, `ListAccounts`, `ListAccountsForParent` e `ListDelegatedAdministrators`, e retornam o mesmo espaço reservado. Não é um endereço de e-mail que você possa usar ou alterar.
- Você não pode atualizar o endereço de e-mail do usuário raiz de uma conta do projeto. As chamadas para `StartPrimaryEmailUpdate` ou `AcceptPrimaryEmailUpdate` para uma conta de projeto falham com um `AccessDeniedException` erro, mesmo quando o chamador tem as permissões necessárias.
- Você não pode entrar em uma conta do projeto como usuário root nem recuperar sua senha de usuário root.
- Você não pode remover uma conta de projeto da sua organização e ela não pode sair da sua organização ou ingressar em outra organização. Se você `RemoveAccountFromOrganization` solicitar uma conta de projeto, a chamada falhará com um `ConstraintViolationException` erro que diz que a conta pertence a uma ID do Builder.

Para parar de usar uma conta de projeto, feche-a da sua conta de gerenciamento. Como você não pode remover contas de projeto da sua organização, você só pode excluir sua organização depois que todas as contas do projeto, incluindo a conta de administrador delegado de identidade, forem encerradas permanentemente. AWS fecha permanentemente uma conta quando seu período de 90 dias após o fechamento termina.

As contas de membros que você cria na sua organização depois de ativar os recursos avançados têm um endereço de e-mail de usuário raiz, e essas diferenças não se aplicam a elas. Se você precisar de uma conta cujo endereço de e-mail do usuário raiz possa ser alterado ou que possa ser removido da sua organização posteriormente, crie uma nova conta de membro e mova seus recursos para ela.

Como será AWS As configurações mudam depois que eu ativo os recursos avançados?

Depois de ativar os recursos avançados, AWS as Configurações estarão disponíveis desde que você use o AWS Builder ID como sua fonte de identidade. AWS As configurações só poderão ser acessadas em <https://settings.aws.com>. Você não poderá acessá-lo a partir do Console de gerenciamento da AWS. AWS As configurações fornecerão links para gerenciar sua conta usando sua conta de gerenciamento. Com sua conta de gerenciamento, você pode acessar os seguintes

Console de gerenciamento da AWS locais em AWS Configurações. Use a conta de gerenciamento somente para realizar tarefas administrativas, incluindo:

- Acesse o Billing and Cost Management Console para ver suas informações de cobrança.
- Acesse o console AWS da organização para modificar os SCPs e RCPs que governam sua organização.
- Acesse o console do AWS Account Access Manager para modificar o acesso refinado às identidades de sua força de trabalho.
- Acesse o IAM Identity Center para alterar sua fonte de identidade.

Use a conta de gerenciamento para realizar essas tarefas. Embora você também tenha acesso ao e-mail e à senha do usuário raiz, recomendamos que você use apenas suas credenciais de usuário raiz para acesso emergencial à sua conta.

Você também pode usar AWS as Configurações para acessar suas AWS contas em sua organização e qualquer projeto compartilhado com você.

Se você quiser criar funções personalizadas e acessá-las AWS nas Configurações de suas contas, defina a duração da sessão para 12 horas.

Se você tiver acesso de um membro da equipe a um projeto, poderá visualizá-lo e acessá-lo da mesma forma que antes de ativar os recursos avançados. Todos os projetos compartilhados com você não serão afetados se você ativar recursos avançados para sua própria conta de gerenciamento e AWS organização.

Ainda posso criar um projeto no AWS Configurações após eu ativar os recursos avançados?

Você não pode criar um projeto na sua AWS organização atual depois de ativar os recursos avançados. Você deve criar uma conta de membro em sua organização.

Você pode criar uma nova AWS organização gerenciada com padrões pré-configurados. Para fazer isso, crie um novo projeto em AWS Configurações. Em seguida, você pode criar projetos adicionais e convidar membros da equipe para colaborar. Você também pode ativar recursos avançados para essa conta de gerenciamento.

O novo ambiente pré-configurado que você acessa não terá conexão com a AWS organização anterior que foi criada quando você se inscreveu pela primeira vez. AWS

Como se preparar para ativar recursos avançados

Recomendamos fazer o seguinte antes de ativar os recursos avançados:

- Informe a todos os membros da sua equipe que você ativará recursos avançados. A menos que você modifique qualquer configuração, os membros da sua equipe terão o mesmo acesso aos projetos, mas as Console de gerenciamento da AWS mudanças mudarão da visualização simplificada para uma visualização que mostra regiões e fornece acesso a mais serviços. Se você alterar posteriormente a fonte de identidade ou adicionar novos SCPs ou RCPs, informe sua força de trabalho, pois essas mudanças podem afetar a forma como eles se conectam e o que podem acessar.
- Veja os gastos de todos os seus projetos atuais e observe se algum projeto contém custos que flutuam significativamente. Sem um limite de gastos, você será responsável por todos os custos incorridos por seus recursos. Recomendamos que você exclua ou pause os recursos ociosos antes de ativar os recursos avançados.
- Planeje as mudanças que você fará em suas AWS organizações e pesquise as melhores práticas. Se você planeja criar recursos em um outro Região da AWS, modifique a política de controle de serviço que é aplicada para restringir todos os usuários Regiões da AWS. Você precisa modificar o StatementID RegionFloor para incluir quaisquer novas regiões. Para obter mais informações, consulte [Políticas de controle de serviços para projetos](#).
- Se você seguiu as etapas [Conecte uma ferramenta de codificação de IA](#), sua ferramenta de IA tem contexto apenas sobre a nova AWS experiência. Isso pode causar problemas à medida que você desenvolve usando recursos avançados. Recomendamos o seguinte:
 - Remova o `aws-starter-rules.md` arquivo do local em que você o salvou. O arquivo de regras foi salvo dependendo do seu agente. Para obter mais informações, consulte [Onde colocar o arquivo de regras](#).

Como ativar recursos avançados

Você pode ativar recursos avançados em AWS Configurações. A ativação não pode ser revertida.

Para ativar recursos avançados

1. Abra AWS as Configurações em <https://settings.aws.com>.
2. No painel de navegação principal, escolha Projetos.
3. Em Ações, escolha Explorar recursos avançados.

Como a ativação não pode ser revertida, daremos mais tempo para explorar e aprender sobre o processo de ativação.

4. Quando estiver pronto para ativar, faça o seguinte:
 - a. Em Nome da equipe, insira o nome da equipe. Esse é o nome da instância do IAM Identity Center usada para armazenar suas identidades de força de trabalho. Sua força de trabalho verá esse nome.
 - b. Em Escolher endereço de e-mail da conta de gerenciamento, escolha um endereço de e-mail. Esse endereço de e-mail é usado para acessar a conta de gerenciamento e realizar tarefas. Se você usar um endereço de e-mail diferente, o e-mail do AWS Builder ID ainda terá acesso à conta de gerenciamento em AWS Configurações, desde que você ainda use o AWS Builder ID como sua fonte de identidade.
 - c. Conclua o processo de verificação do endereço de e-mail da conta de gerenciamento.
 - d. Escolha Revisar e conclua a ativação.
 - e. Confirme sua escolha e escolha ativar. Se você fizer isso, não poderá reverter sua conta.

Parabéns, você ativou AWS recursos avançados!

Depois de ativar os recursos avançados

Depois de ativar os recursos avançados, você pode fazer o seguinte:

- [Gerencie membros da força de trabalho](#)
- [Alterar fonte de identidade de AWS ID do builder](#)
- [Remover políticas da organização](#)
- [Crie uma unidade organizacional](#)
- [Ativar ou desativar Regiões da AWS em sua conta](#)
- [Crie funções do IAM](#)

Defina uma senha de usuário root para sua conta de gerenciamento

Warning

No momento, estamos lançando nossa nova experiência para um número limitado de clientes. Talvez você ainda não consiga acessar essa experiência.

Depois de ativar os recursos avançados, sua conta de gerenciamento agora usa um endereço de e-mail raiz para a recuperação da conta. Embora você ainda possa recuperar o acesso ao seu AWS Builder ID usando [as opções de autoatendimento para recuperar o acesso](#), agora você recupera o acesso à sua conta de gerenciamento com as credenciais do usuário raiz. Para acessar o usuário root, você precisa criar uma senha de usuário root. Além disso, recomendamos que você ative a autenticação multifator (MFA) para aumentar a segurança do usuário root.

Para definir uma senha de usuário root

1. Abra o [AWS Management Console](#) e escolha Entrar usando o e-mail do usuário root.
2. Em Endereço de e-mail, insira o endereço de e-mail do usuário raiz.

Esse é o endereço de e-mail que você definiu para a conta de gerenciamento ao ativar os recursos avançados.

3. Escolha Esqueceu sua senha?.

O processo de redefinição de senha também é a forma como você define sua senha de usuário root depois de ativar os recursos avançados.

4. Insira o endereço de e-mail associado à conta.
5. Forneça o texto CAPTCHA e escolha Não sou um robô.
6. Verifique se há uma mensagem da Amazon Web Services no e-mail Conta da AWS associado a você. O e-mail será enviado por um endereço que termina em `@verify.signin.aws`. Siga as instruções no e-mail para definir uma senha de usuário root. Se você não vir o e-mail em sua conta, verifique a pasta de spam. Se você não tiver mais acesso ao e-mail, consulte [Não tenho acesso ao e-mail da minha AWS conta](#) no Guia do AWS Sign-In usuário.

Depois de definir a senha do usuário root, você pode recuperar o acesso à sua conta. Em seguida, siga as orientações em [Multi-factor autenticação do usuário raiz da AWS conta para](#) ativar o MFA para suas credenciais raiz.

Use somente o usuário root para recuperar sua conta ou, quando necessário, para realizar [tarefas que exijam credenciais de usuário root](#). Para o trabalho diário, faça login com sua fonte de identidade, como AWS Builder ID.

Gerencie membros da força de trabalho

Warning

No momento, estamos lançando nossa nova experiência para um número limitado de clientes. Talvez você ainda não consiga acessar essa experiência.

Depois de ativar os recursos avançados, você pode convidar novos membros da força de trabalho ou remover membros existentes da força de trabalho. Isso inclui adicionar sua força de trabalho existente a novas AWS contas. As informações a seguir são somente para AWS organizações que usam o AWS Builder ID como fonte de identidade. Se você usa um provedor de identidade externo (IdP), gerencia sua força de trabalho nesses provedores de identidade. Se você usa o diretório do Identity Center, use a documentação descrita em [Gerenciar usuários no diretório do Identity Center](#).

Para convidar novos membros da força de trabalho

1. Abra AWS as Configurações em <https://settings.aws.com>.
2. No painel de navegação principal, escolha Projetos.
3. Visite o AWS console da sua conta de administrador delegada de identidade.
4. Na página inicial do AWS console, pesquise **IAM Identity Center** e escolha.
5. Na página Usuários do console do IAM Identity Center, escolha Convidar novo membro da equipe.
6. Em E-mail, insira um endereço de e-mail ou uma lista de endereços de e-mail. Separe os endereços de e-mail com vírgulas (,) ou ponto e vírgula (;).
7. Selecione Enviar convite.

Para conceder a um novo membro da força de trabalho acesso a AWS contas

Depois que o membro da força de trabalho aceitar o convite, você configura AWS as contas às quais ele tem acesso.

Conceda permissões completas a uma conta que você criou antes de ativar os recursos avançados

1. Identifique o ID da conta à qual você deseja conceder acesso. Para encontrar o ID da conta, consulte [Exibir identificadores AWS da conta](#).
2. No painel de navegação principal, escolha Grupos.
3. Selecione o nome do grupo que começa com o ID da conta que você identificou.
4. Escolha Adicionar usuários ao grupo.
5. Selecione o usuário que você deseja adicionar.
6. Escolha Adicionar 1 usuário.

Conceda permissões personalizadas a um novo ou existente AWS account

Você configura o acesso personalizado no AWS Account Access Manager. Para obter mais informações, consulte [Gerenciar o acesso às AWS contas](#).

 Note

Se você quiser criar funções personalizadas e conceder acesso a elas AWS nas Configurações, defina a duração da sessão para 12 horas.

Para remover membros da força de trabalho

1. Abra AWS as Configurações em <https://settings.aws.com>.
2. No painel de navegação principal, escolha Projetos.
3. Em Ações, escolha Gerenciar equipe.

Isso abrirá o IAM Identity Center.

4. Na página Usuários do console do IAM Identity Center, selecione um membro da equipe e escolha Remover.
5. Confirme sua escolha e escolha Remover.

O membro da equipe perderá imediatamente todo o acesso à sua AWS organização.

Essas etapas mostram como gerenciar os membros da sua força de trabalho acessando primeiro AWS as Configurações. No entanto, você pode fazer login Console de gerenciamento da AWS com

sua conta de administrador delegado e acessar o IAM Identity Center ou o console do IAM para gerenciar os membros da sua força de trabalho.

Alterar fonte de identidade de AWS ID do builder

Warning

No momento, estamos lançando nossa nova experiência para um número limitado de clientes. Talvez você ainda não consiga acessar essa experiência.

Depois de ativar os recursos avançados, você pode alterar sua fonte de identidade a partir do AWS Builder ID. Se você alterar sua fonte de identidade do AWS Builder ID, nunca poderá reutilizar o AWS Builder ID como a fonte de identidade da sua AWS organização. Alterar sua fonte de identidade muda a forma como sua força de trabalho faz login. Seu ID do AWS Builder continua sendo proprietário de suas contas de projeto.

Para alterar sua fonte de identidade de AWS ID do builder

1. Abra AWS as Configurações em <https://settings.aws.com>.
2. No painel de navegação principal, escolha Projetos.
3. Em Gerenciar esta organização, escolha Alterar fonte de identidade.

Isso abrirá o IAM Identity Center.

4. Na página Configurações do console do IAM Identity Center, escolha Ações e, em seguida, Alterar fonte de identidade.
5. Em Escolher fonte de identidade, a ID do AWS Construtor será selecionada. Escolha uma nova fonte e, em seguida, escolha Avançar.
6. Se você estiver mudando para o Active Directory, escolha o diretório disponível no menu na próxima página. Se você estiver migrando para um provedor de identidade externo, recomendamos que siga as etapas em [Como se conectar a um provedor de identidade externo](#).
7. Revise e confirme suas alterações. Você precisará marcar todas as caixas de seleção para confirmar que entendeu as mudanças em sua organização.
8. Confirme sua escolha e escolha Alterar fonte de identidade.

Essas etapas mostram como alterar sua fonte de identidade acessando primeiro AWS as Configurações. No entanto, você pode entrar no Console de gerenciamento da AWS com sua conta de administrador delegado e acessar o IAM Identity Center para alterar sua fonte de identidade.

Remover políticas da organização

Warning

No momento, estamos lançando nossa nova experiência para um número limitado de clientes. Talvez você ainda não consiga acessar essa experiência.

Depois de ativar os recursos avançados, você pode modificar as Políticas de Controle de Recursos (RCPs) e as Políticas de Controle de Serviços (SCPs) para alterar a governança da sua organização. AWS Certas políticas organizacionais AWS gerenciadas são removidas quando você ativa recursos avançados. Para obter mais informações, consulte [Políticas gerenciadas para sua organização](#). As informações a seguir são somente para AWS organizações que usam o AWS Builder ID como fonte de identidade. Se você usa outra fonte, siga as etapas em [Atualizar uma política](#).

Para modificar uma política de controle de serviços (SCP)

1. Abra AWS as configurações em <https://settings.aws.com>.
2. No painel de navegação principal, escolha Projetos.
3. Em Gerenciar esta organização, escolha Gerenciar políticas.

Isso abrirá o AWS Organizations console.

4. Escolha a página Política de controle de serviços.
5. Escolha o nome da política que você deseja atualizar.
6. Na página de detalhes da política, escolha Edit policy (Editar política).
7. Faça uma ou todas as alterações a seguir:
 - Você pode renomear a política inserindo um novo nome em Policy name (Nome da política).
 - Você pode alterar a descrição inserindo o novo texto em Policy description (Descrição da política).
 - Você pode editar o texto da política editando a política no formato JSON no painel esquerdo. Como alternativa, você pode escolher uma instrução no editor à direita e também alterar seus

elementos usando os controles. Para obter mais detalhes sobre cada controle, consulte Criar um procedimento de SCP anteriormente neste tópico.

8. Ao concluir, escolha Salvar alterações.

Para modificar uma política de controle de recursos (RCP)

1. Abra AWS as configurações em <https://settings.aws.com>.
2. No painel de navegação principal, escolha Projetos.
3. Em Gerenciar esta organização, escolha Gerenciar políticas.

Isso abrirá o AWS Organizations console.

4. Escolha a página Política de controle de recursos.
5. Escolha o nome da política que você deseja atualizar.
6. Na página de detalhes da política, escolha Edit policy (Editar política).
7. Faça uma ou todas as alterações a seguir:
 - Você pode renomear a política inserindo um novo nome em Policy name (Nome da política).
 - Você pode alterar a descrição inserindo o novo texto em Policy description (Descrição da política).
 - Você pode editar o texto da política editando a política no formato JSON no painel esquerdo. Como alternativa, você pode escolher uma instrução no editor à direita e também alterar seus elementos usando os controles. Para obter mais detalhes sobre cada controle, consulte Criar um procedimento de RCP anteriormente neste tópico.
8. Ao concluir, escolha Salvar alterações.

Essas etapas mostram como modificar as políticas da organização por meio das AWS Configurações. No entanto, você pode entrar no Console de gerenciamento da AWS com sua conta de gerenciamento e acessar o AWS Organizations console para modificar essas políticas.

Feche sua conta em AWS Configurações

Warning

No momento, estamos lançando nossa nova experiência para um número limitado de clientes. Talvez você ainda não consiga acessar essa experiência.

Se você não precisar mais da organização e de todos os projetos armazenados nela, você poderá fechar seus projetos, fechar sua conta de gerenciamento e excluir sua ID do AWS Builder.

Para garantir que você não seja mais cobrado pelos AWS recursos que consome, você deve fechar seus projetos e fechar a conta de gerenciamento da sua organização, mas não precisa fechar seu AWS perfil. Seu ID de AWS construtor associado a ele é gratuito.

Depois de fechar sua conta de gerenciamento, você poderá reabri-la em até 90 dias a partir do dia em que a fechou. O tempo entre o dia em que você fechou a conta de gerenciamento e o encerramento AWS permanente da conta de gerenciamento é o período pós-encerramento.

O que você precisa saber antes de fechar sua conta de gerenciamento

Antes de fechar sua conta de gerenciamento, você deve considerar o seguinte:

- Ao fechar um projeto, considere as considerações em [O que você precisa saber antes de fechar seu projeto](#).
- Você deve fechar todos os projetos antes de fechar sua conta de gerenciamento.
- Você deve fechar sua conta de gerenciamento antes de excluir seu AWS Builder ID.
- Depois de fechar sua conta de gerenciamento, você poderá reabri-la em até 90 dias a partir do dia em que a fechou. O tempo entre o dia em que você fechou a conta de gerenciamento e o encerramento AWS permanente da conta de gerenciamento é o período pós-encerramento.
- Você pode reabrir a conta durante o período pós-encerramento.
- Você não pode usar o mesmo endereço de e-mail que estava registrado na sua organização no momento do encerramento como e-mail principal de outra organização. Se você quiser usar o mesmo endereço de e-mail para uma organização diferente ao usar o Sign up for AWS (new), recomendamos atualizá-lo antes do encerramento. Para obter mais informações, consulte [Altere seu endereço de e-mail em AWS Configurações](#).

- Se você ativou a autenticação multifator (MFA) em sua conta de gerenciamento e configurou um dispositivo de MFA, a MFA não é removida automaticamente quando você fecha a conta de gerenciamento. Se você optar por deixar a MFA ativada durante o período pós-encerramento de 90 dias, mantenha o dispositivo com MFA ativo até que o período pós-encerramento expire, caso você precise acessar a conta durante esse período. Observe que os dispositivos token TOTP de hardware não podem ser associados a outro usuário após o encerramento permanente da conta. Se quiser usar o token TOTP de hardware com outro usuário posteriormente, você tem a opção de desativar o dispositivo MFA de hardware antes de fechar a conta de gerenciamento.

Fechar um projeto

Para fechar seus projetos, consulte [Fechar um projeto em AWS Configurações](#).

Feche sua conta de gerenciamento

Para fechar sua conta de gerenciamento

1. Abra AWS as configurações em <https://settings.aws.com>.
2. No painel de navegação principal, escolha Projeto.
3. Em Ações, escolha Fechar conta de gerenciamento.
4. Confirme sua escolha e escolha Fechar conta de gerenciamento.

Exclua seu AWS ID do builder

A exclusão do seu AWS Builder ID resultará no seguinte:

- Perda de acesso: além de seu projeto e organização, você não pode mais acessar nenhuma AWS ferramenta e serviço que você acessou anteriormente por meio do AWS Builder ID.
- Exclusão de conteúdo: qualquer conteúdo restante associado exclusivamente à sua AWS Builder ID será excluído e você não poderá mais acessar ou recuperar seu conteúdo de aplicativos usando sua AWS Builder ID.
- Exclusão de informações pessoais: todas as informações pessoais que você forneceu em conexão com a criação e administração de sua ID do AWS Builder serão excluídas, exceto que AWS possam reter informações pessoais conforme exigido ou permitido por lei, como registros de sua solicitação de exclusão ou dados em um formulário que não o identifique.

Você pode descobrir mais sobre como lidamos com suas informações no Aviso AWS de Privacidade. Você pode atualizar suas preferências de AWS comunicação ou cancelar a assinatura visitando o Centro de Preferências de AWS Comunicação.

Os logins existentes permanecem inalterados — Se você estiver usando um login como Google ou Apple, excluir seu AWS Builder ID não exclui nada relacionado à sua conta de login.

Para excluir seu AWS ID do builder

1. Abra AWS as configurações em <https://settings.aws.com>.

Mesmo que você tenha excluído sua conta de gerenciamento, você ainda pode entrar.

2. No painel de navegação principal, escolha Gerenciar perfil.
3. Para informações do perfil, escolha Gerenciar perfil.

Você será redirecionado para o seu perfil AWS Builder ID.

4. No painel de navegação principal, escolha Privacidade e dados.
5. Para Excluir ID do AWS Builder, escolha Excluir seu ID do AWS Builder.
6. Confirme sua escolha e selecione Excluir.

Inscriva-se para AWS (avançado)

Se você é novo em AWS, a primeira etapa é se inscrever em um Conta da AWS. Quando você segue as informações de Inscrever-se em AWS (avançado), AWS cria uma conta na qual você tem controle total sobre a configuração da conta e onde seu conteúdo é armazenado. Use essa opção se você tiver cargas de trabalho regulamentadas, como HIPAA, FedRAMP.

Para comparar essa inscrição com Inscrever-se em AWS (novo), consulte [Compare as opções de inscrição](#).

Para se inscrever em um Conta da AWS, você precisará fornecer as seguintes informações:

- **Endereço de e-mail do usuário-raiz:** esse endereço de e-mail é usado como nome de login do [usuário-raiz](#) e é necessário para a recuperação da conta. Você precisa poder receber mensagens de e-mail que sejam enviadas para esse endereço. Antes de poder executar determinadas tarefas, você precisa verificar se tem acesso a e-mails enviados para esse endereço.
- **AWS nome da conta** — O nome da conta aparece em vários lugares, como na sua fatura, e em consoles, como o painel Billing and Cost Management e o console. AWS Organizations Recomendamos que você use uma forma padrão de dar nome às contas para poder dar nomes fáceis de reconhecer. Para contas corporativas, considere usar um padrão de nomenclatura, como organização - propósito - ambiente (por exemplo, AnyCompany- auditoria - produção). Em contas pessoais, considere usar um padrão de nomenclatura, como nome-sobrenome-finalidade (por exemplo, paulo-santos-contateste).
- **Endereço** — Se seu endereço de contato e cobrança for na Índia, o contrato de usuário da sua conta é com a Amazon Web Services India Private Limited (AWS Índia), um vendedor AWS local na Índia. É necessário fornecer o CVV como parte do processo de verificação. Talvez você também precise inserir uma senha de uso único, dependendo do seu banco. AWS A Índia cobra 2 INR de sua forma de pagamento como parte do processo de verificação. AWS A Índia reembolsa os 2 INR após a conclusão da verificação.
- **Número de telefone:** esse número é usado para fins de verificação de identidade e para confirmar a propriedade da conta. Ele precisa estar disponível para receber chamadas e mensagens de SMS.

 Important

Se essa conta for para uma empresa, use um número de telefone corporativo para que sua empresa possa manter o acesso a ela Conta da AWS mesmo quando um funcionário mudar de cargo ou sair da empresa.

Etapa 1: criar a conta

Essas instruções são para criar um ambiente Conta da AWS fora da Índia. Para criar uma conta na Índia, consulte [Crie um Conta da AWS por AWS Índia](#). Para criar uma conta que faz parte de uma organização gerenciada por AWS Organizations, consulte [Criação de uma conta de membro em uma organização](#) no Guia AWS Organizations do usuário.

Console de gerenciamento da AWS

Para criar um Conta da AWS

1. Abra a página [Cadastrar-se na AWS](#).
2. Insira o endereço de e-mail e o Conta da AWS nome do usuário raiz e escolha Verificar endereço de e-mail. Isso envia um código de verificação para seu endereço de e-mail.

 Important

Se essa conta for para uma empresa, use uma lista de distribuição corporativa segura (por exemplo, `it.admins@example.com`) para que sua empresa possa manter o acesso a ela Conta da AWS mesmo quando um funcionário mudar de cargo ou sair da empresa. Como o endereço de e-mail pode ser usado para redefinir as credenciais do usuário-raiz da conta, proteja o acesso a essa lista de distribuição ou endereço.

3. Insira seu código de verificação e escolha Verificar.
4. Insira uma senha forte para seu usuário root, confirme-a e escolha Continuar. AWS exige que sua senha atenda às seguintes condições:
 - Ter no mínimo 8 caracteres e no máximo 128 caracteres de extensão.

- Incluir no mínimo três dos seguintes tipos de caracteres: maiúsculas, minúsculas, números e os símbolos ! @ # \$ % ^ & * () < > [] { } | _ + - =.
 - Não deve ser idêntico ao seu Conta da AWS nome ou endereço de e-mail.
5. Escolha o plano da sua conta. Para obter mais informações, consulte [Planos de nível gratuito](#).
 6. Insira suas informações de contato e, em seguida, leia e aceite o [Contrato AWS do Cliente](#). Certifique-se de entender os termos antes de aceitar.

 Important

Se essa conta for para uma empresa, é uma prática recomendada inserir o número de telefone da empresa em vez do número de um telefone pessoal. Configurar o usuário-raiz da conta com um endereço de e-mail individual ou um número de telefone pessoal pode tornar a conta insegura.

7. Insira suas informações de cobrança. Se você quiser usar um endereço de cobrança diferente para suas informações de AWS cobrança, escolha Usar um novo endereço.

Você não poderá continuar com o processo de cadastro até adicionar um método de pagamento válido.

8. Talvez seja necessário confirmar sua identidade:
 - a. Em Código do país ou região, insira um número de telefone que possa ser contatado nos próximos minutos.
 - b. Em Número de telefone, insira um número de telefone que possa ser acessado nos próximos minutos.
 - c. Escolha Enviar SMS.
 - d. Quando o sistema automatizado entrar em contato com você, insira o código recebido e escolha Continuar.
9. Escolha um dos AWS Support planos disponíveis. Para obter uma descrição dos planos de suporte disponíveis e seus benefícios, consulte [Comparar planos Suporte](#).
10. Escolha Concluir cadastramento. É exibida uma página de confirmação indicando que sua conta está sendo ativada.

11. Verifique suas pastas de e-mail e de spam para encontrar uma mensagem de e-mail que confirme sua conta foi ativada. A ativação geralmente leva alguns minutos mas, às vezes, pode demorar até 24 horas.
12. Depois de receber a mensagem de ativação, você pode entrar no para começar a [Console de gerenciamento da AWS](#)usar. Serviços da AWS Para obter informações gerais sobre como gerenciar suas configurações de conta, consulte [Configure seu Conta da AWS](#).

Para vários Contas da AWS gerenciados AWS Organizations, atribua acesso administrativo a um usuário administrativo no IAM Identity Center. Para obter instruções, consulte [Configurar o Conta da AWS acesso para um usuário administrativo do IAM Identity Center](#) no Guia do usuário do IAM Identity Center.

AWS CLI & SDKs

Você pode criar contas de membros em uma organização gerenciada AWS Organizations executando a [CreateAccount](#) operação enquanto estiver conectado à conta de gerenciamento da organização.

Você não pode criar uma operação autônoma Conta da AWS fora de uma organização usando uma operação AWS Command Line Interface (AWS CLI) ou de AWS API.

Etapa 2: (recomendado) instalar o AWS CLI

Instale o AWS CLI seguindo as instruções em [Instalando AWS CLI](#) o. Você precisa da versão 2.32.0 ou posterior.

Você pode usar o AWS CLI para que um agente gerencie AWS recursos em seu nome.

Depois de instalar o AWS CLI, use o comando a seguir para fazer login programaticamente:

```
aws login
```

Isso alterna automaticamente suas credenciais a cada 15 minutos, mantendo sua sessão válida por até 12 horas sem intervenção manual.

Use o comando a seguir para verificar se suas credenciais estão funcionando:

```
aws sts get-caller-identity
```

Para obter mais informações sobre como acessar seu Conta da AWS, consulte [Acessando seu Conta da AWS](#).

Etapa 3: (Recomendado) Configurar o AWS Servidor MCP

O AWS MCP Server é um servidor gerenciado que dá acesso aos agentes AWS por meio do Model Context Protocol (MCP). Os agentes podem pesquisar a AWS documentação e recuperar informações do serviço sem autenticação. Para executar chamadas de AWS API, executar scripts Python em um ambiente de sandbox ou seguir habilidades selecionadas, os agentes se autenticam por meio de suas credenciais existentes do IAM. Para obter mais informações, consulte [O que é o kit de ferramentas do AWS agente?](#)

Depois de concluir o processo de inscrição, consulte os tópicos a seguir:

- [Relacionado AWS serviços](#)
- [Usar o Usuário raiz da conta da AWS](#)
- [Acessando seu Conta da AWS](#)
- [Planeje seu Conta da AWS estrutura de governança](#)
- [Configure seu Conta da AWS](#)
- [Solucione o problema do seu Conta da AWS](#)
- [Gerenciar contas na Índia](#)
- [Fechar um Conta da AWS](#)
- [Reabrir um Conta da AWS](#)

Relacionado AWS serviços

Dependendo de como você se inscreve AWS, você tem acesso aos Contas da AWS nossos projetos. Os projetos contêm Contas da AWS e as configurações para compartilhar com outros colaboradores. Para obter mais informações, consulte [Compare as opções de inscrição](#). Nesta seção, explicamos como Contas da AWS você cria usando o Sign up for AWS (avançado) para funcionar perfeitamente com os seguintes serviços:

- IAM

Seu Conta da AWS está intimamente integrado ao AWS Identity and Access Management (IAM). Você pode usar o IAM com a conta para garantir que outras pessoas que trabalham na conta

tenham o acesso necessário para a conclusão dos seus trabalhos. Você também usa o IAM para controlar o acesso a todos os seus AWS recursos, não apenas às informações específicas da conta. É importante que você se familiarize com os principais conceitos e com as práticas recomendadas do IAM antes de avançar muito na configuração da estrutura da Conta da AWS. Para obter mais informações, consulte [Práticas recomendadas de segurança no IAM](#) no Guia do usuário do IAM.

- AWS Organizations

Se sua empresa é grande ou tem probabilidade de crescer, convém configurar várias AWS contas que reflitam a estrutura específica da sua empresa. AWS Organizations fornece a infraestrutura e os recursos subjacentes para você criar e gerenciar seus ambientes com várias contas. Você pode combinar suas contas existentes em uma organização que permite gerenciar as contas de forma centralizada. Você pode criar contas que automaticamente façam parte de sua organização e convidar outras contas para ingressar nela. Você também pode anexar políticas que afetam algumas ou todas as suas contas. Para obter mais informações, consulte [Quando usar AWS Organizations](#).

As seguintes ações de API relacionadas à conta fazem parte da AWS Organizations API, não da API de gerenciamento de AWS contas. Nós as incluímos aqui porque os clientes geralmente procuram essas operações na documentação de gerenciamento de contas, mas elas são definidas no AWS Organizations namespace.

- [CreateAccount](#)
- [CreateGovCloudAccount](#)
- [DescribeAccount](#)

- AWS Control Tower

AWS Control Tower fornece uma maneira simplificada de configurar e controlar um ambiente seguro com várias contas AWS. AWS Control Tower automatiza a criação de seu ambiente de várias contas usando AWS Organizations, instanciando um conjunto de contas iniciais e com algumas barreiras e configurações padrão para o ambiente. Você pode usar AWS Control Tower para provisionar novas Contas da AWS em algumas etapas e, ao mesmo tempo, garantir que as contas estejam em conformidade com suas políticas organizacionais. Para obter mais informações, consulte [Quando usar AWS Control Tower](#).

Usar o Usuário raiz da conta da AWS

Dependendo de como você se inscreve AWS, você tem acesso aos Contas da AWS projetos. Os projetos contêm Contas da AWS as configurações para compartilhamento com outros colaboradores. Para obter mais informações, consulte [Compare as opções de inscrição](#). Nesta seção, explicamos como usar o usuário root em um Conta da AWS que você cria usando o Sign up for AWS (avançado). Uma ID do AWS Builder é proprietária de cada conta do projeto em vez do endereço de e-mail do usuário raiz, então você não pode usar o usuário raiz em uma conta do projeto, inclusive depois de ativar os recursos avançados.

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.

Para evitar o uso do usuário-raiz nas tarefas diárias, saiba como [configurar um usuário administrativo no Centro de Identidade do AWS IAM](#). Para obter mais recomendações de segurança do usuário raiz, consulte [As práticas recomendadas do usuário raiz para a Conta da AWS](#).

Important

Qualquer pessoa que tenha suas credenciais de usuário root Conta da AWS tem acesso irrestrito a todos os recursos da sua conta, incluindo informações de cobrança.

Você pode [alterar](#) ou [redefinir a senha do usuário-raiz](#) e [criar](#) ou [excluir chaves de acesso](#) (IDs de chave de acesso e chaves de acesso secretas) para o usuário-raiz. Para obter ajuda para fazer login usando seu usuário root, consulte [Fazer login Console de gerenciamento da AWS como usuário root no Guia do AWS Sign-In usuário](#).

Acessando seu Conta da AWS

Essas informações são sobre como acessar você Conta da AWS se inscreveu para AWS usar o Sign up for AWS (avançado) ou se tiver ativado recursos avançados para sua conta. Para comparar as opções de inscrição, consulte [Compare as opções de inscrição](#).

Você pode acessar o seu Conta da AWS de qualquer uma das seguintes formas:

Console de gerenciamento da AWS

[Console de gerenciamento da AWS](#) É uma interface baseada em navegador que você pode usar para gerenciar suas Conta da AWS configurações e seus AWS recursos.

AWS Ferramentas de linha de comando

Com as ferramentas de linha de AWS comando, você pode emitir comandos na linha de comando do seu sistema para executar Conta da AWS AWS tarefas. Usar a linha de comando pode ser mais rápido e mais conveniente do que o console. As ferramentas de linha de comando também são úteis se você quiser criar scripts que executam AWS tarefas. AWS fornece dois conjuntos de ferramentas de linha de comando:

- [AWS Command Line Interface](#)(AWS CLI). Para obter informações sobre como instalar e usar o AWS CLI, consulte o Guia [AWS Command Line Interface do usuário](#).
- [AWS Tools for Windows PowerShell](#). Para obter informações sobre como instalar e usar as Ferramentas para Windows PowerShell, consulte o Guia [Ferramentas da AWS para PowerShell do usuário](#).

AWS SDKs

Os AWS SDKs consistem em bibliotecas e códigos de amostra para várias linguagens e plataformas de programação (por exemplo, Java, Python, Ruby, .NET, iOS e Android). Os SDKs processam tarefas como assinatura criptográfica de solicitações, gerenciamento de erros e novas tentativas automáticas de solicitações. Para obter mais informações sobre os AWS SDKs, incluindo como baixá-los e instalá-los, consulte [Ferramentas para a Amazon Web Services](#).

AWS API de consulta HTTPS de gerenciamento de contas

A API de consulta HTTPS de gerenciamento de AWS contas oferece acesso programático ao seu Conta da AWS e. AWS A API de consulta HTTPS permite que você execute solicitações HTTPS diretamente para o serviço. Quando você usa a API HTTPS, deve incluir código para assinar digitalmente solicitações usando suas credenciais. Para obter mais informações, consulte [Calling the API by making HTTP Query requests](#).

Planeje seu Conta da AWS estrutura de governança

Essas informações são sobre o planejamento de sua estrutura de Conta da AWS governança se você se inscreveu para AWS usar o Sign up for AWS (avançado) ou se tiver ativado recursos avançados para sua conta. Para comparar as opções de inscrição, consulte [Compare as opções de inscrição](#).

Embora você possa ter iniciado sua AWS jornada com uma única conta, AWS recomenda configurar várias contas à medida que suas cargas de trabalho aumentam em tamanho e complexidade. Se você é uma empresa de médio ou de grande porte, convém criar um plano de estrutura de governança que garanta que as necessidades de dados e de workload sejam atendidas.

Esta seção aborda os benefícios e os serviços de governança disponíveis AWS para ajudar a habilitar uma estrutura de governança com várias contas.

Tópicos

- [Benefícios do uso de vários Contas da AWS](#)
- [Quando usar AWS Organizations](#)
- [Quando usar AWS Control Tower](#)
- [Noções básicas dos modos de operação da API](#)

Benefícios do uso de vários Contas da AWS

Essas informações são sobre os benefícios de usar vários Contas da AWS se você se inscreveu para AWS usar o Sign up for AWS (avançado) ou se tiver ativado recursos avançados para sua conta. Para comparar as opções de inscrição, consulte [Compare as opções de inscrição](#).

Contas da AWS formam o limite de segurança fundamental no. Nuvem AWS Elas atuam como um contêiner para recursos, fornecendo uma camada crítica de isolamento que é essencial para a criação de um ambiente seguro e bem governado. Para obter mais informações, consulte [O que é um Conta da AWS?](#).

Separar seus recursos em separados Contas da AWS ajuda você a apoiar os seguintes princípios em seu ambiente de nuvem:

- **Controle de segurança:** aplicações diferentes podem ter perfis de segurança diferentes, exigindo políticas e mecanismos de controle diferentes. Por exemplo, é muito mais fácil conversar com um auditor e apontar para um único Conta da AWS que hospede todos os elementos de sua carga de trabalho sujeitos aos padrões de segurança do setor de cartões de [pagamento \(PCI\)](#).
- **Isolamento** — An Conta da AWS é uma unidade de proteção de segurança. Os riscos potenciais e as ameaças à segurança devem estar contidos dentro e Conta da AWS sem afetar os outros. Pode haver necessidades de segurança diferentes devido a equipes ou perfis de segurança diferentes.

- Muitas equipes — equipes diferentes têm responsabilidades e necessidades de recursos diferentes. Você pode evitar que as equipes interfiram umas nas outras movendo-as para uma posição separada Contas da AWS.
- Isolamento de dados — Além de isolar as equipes, é importante isolar os armazenamentos de dados em uma conta. Isso pode ajudar a limitar o número de pessoas que podem acessar e gerenciar esse armazenamento de dados. Isso ajuda a conter a exposição a dados altamente privados e, portanto, pode ajudar na conformidade com o [Regulamento Geral de Proteção de Dados \(GDPR\) da União Europeia](#).
- Processo de negócios — Diferentes unidades de negócios ou produtos podem ter finalidades e processos completamente diferentes. Com várias Contas da AWS, você pode atender às necessidades específicas de uma unidade de negócios.
- Faturamento — Uma conta é a única maneira verdadeira de separar itens em um nível de faturamento. Várias contas ajudam a separar itens em um nível de cobrança entre unidades de negócios, equipes funcionais ou usuários individuais. Você ainda pode consolidar todas as suas faturas em um único pagador (usando AWS Organizations e consolidando o faturamento) enquanto tem os itens de linha separados por. Conta da AWS
- Alocação de cotas — as cotas AWS de serviço são aplicadas separadamente para cada uma. Conta da AWS Separar as workloads em diferentes Contas da AWS impede que elas consumam cotas umas das outras.

Todas as recomendações e procedimentos descritos neste documento estão em conformidade com a [AWS Well-Architected Estrutura](#). Essa estrutura tem como objetivo ajudar você a projetar uma infraestrutura de nuvem flexível, resiliente e escalável. Mesmo quando você está começando aos poucos, recomendamos que prossiga de acordo com estas orientações da estrutura. Isso pode ajudar a escalar seu ambiente com segurança e sem afetar suas operações contínuas à medida que a empresa cresce.

Gerenciando vários Contas da AWS

Antes de começar a adicionar várias contas, você deve desenvolver um plano para gerenciá-las. Para isso, recomendamos que você use [AWS Organizations](#), que é um AWS serviço gratuito para gerenciar tudo Contas da AWS em sua organização.

AWS também oferece AWS Control Tower, que adiciona camadas de automação AWS gerenciada às organizações e a integra automaticamente a outros AWS serviços AWS CloudTrail AWS Config, como Amazon CloudWatch e outros. AWS Service Catalog Esses serviços podem incorrer em custos adicionais. Para obter mais informações, consulte [Preços do AWS Control Tower](#).

Consulte também

- [Quando usar AWS Organizations](#)
- [Quando usar AWS Control Tower](#)

Quando usar AWS Organizations

Essas informações são sobre quando usar AWS Organizations se você se inscreveu para AWS usar o Sign up for AWS (avançado) ou se tiver ativado recursos avançados para sua conta. Para comparar as opções de inscrição, consulte [Compare as opções de inscrição](#).

AWS Organizations é um AWS serviço que você pode usar para gerenciar seu Contas da AWS grupo. Isso fornece recursos, como faturamento consolidado, em que todas as faturas das contas são agrupadas e administradas por um pagante. Você também pode gerenciar de forma centralizada a segurança da organização usando controles baseados em políticas. Para obter mais informações sobre AWS Organizations, consulte o Guia [AWS Organizations do usuário](#).

Acesso confiável

Quando você usa AWS Organizations para gerenciar suas contas como um grupo, a maioria das tarefas administrativas da organização pode ser executada somente pela conta de gerenciamento da organização. Por padrão, isso só inclui as operações relacionadas ao gerenciamento da própria organização. Você pode estender essa funcionalidade adicional para outros AWS serviços, permitindo o acesso confiável entre as organizações e esse serviço. O acesso confiável concede permissões ao AWS serviço especificado para acessar informações sobre a organização e as contas que ela contém. Quando você habilita o acesso confiável para o Gerenciamento de Contas, o serviço de Gerenciamento de Contas concede ao Organizations e à conta de gerenciamento dele permissões para acessar os metadados, como as informações de contato primário ou alternativo, de todas as contas-membro da organização.

Para obter mais informações, consulte [Habilite o acesso confiável para AWS Gerenciamento de contas](#).

Administrador delegado

Depois de habilitar o acesso confiável, você também pode escolher designar uma de suas contas de membro como uma conta de administrador delegada para o gerenciamento de AWS contas. Isso permite que a conta de administrador delegado execute as mesmas tarefas de gerenciamento de metadados do Gerenciamento de Contas para as contas-membro na organização que,

anteriormente, somente a conta de gerenciamento podia fazer. A conta de administrador delegado só pode acessar as tarefas de gerenciamento do serviço de Gerenciamento de Contas. A conta de administrador delegado não tem todo o acesso administrativo à organização que a conta de gerenciamento tem.

Para obter mais informações, consulte [Habilitar uma conta de administrador delegada para AWS Gerenciamento de contas](#).

Políticas de controle de serviço

Quando você Conta da AWS faz parte de uma organização gerenciada por AWS Organizations, o administrador da organização pode aplicar políticas de controle de [serviços \(SCPs\)](#) que podem limitar o que os diretores nas contas dos membros podem fazer. Uma SCP nunca concede permissões; em vez disso, ela é um filtro que limita quais permissões podem ser usadas pela conta-membro. Um usuário ou perfil (uma entidade principal) de uma conta-membro só pode executar as operações que estão na interseção do que é permitido pelas SCPs que se aplicam à conta e pelas políticas de permissão do IAM anexadas à entidade principal. Por exemplo, você pode usar SCPs para impedir que qualquer entidade principal de uma conta modifique os contatos alternativos da própria conta.

Por exemplo, SCPs que se Contas da AWS aplicam a [Restrinja o acesso usando AWS Organizations políticas de controle de serviço](#)

Habilite o acesso confiável para AWS Gerenciamento de contas

Essas instruções explicam como habilitar o acesso confiável para o gerenciamento de AWS contas se você se inscreveu para AWS usar o Sign up for AWS (avançado) ou se tiver ativado recursos avançados para sua conta. Para comparar as opções de inscrição, consulte [Compare as opções de inscrição](#).

Habilitar o acesso confiável para o Gerenciamento de AWS Contas permite que o administrador da conta de gerenciamento modifique as informações e os metadados (por exemplo, detalhes de contato primários ou alternativos) específicos de cada conta de membro em AWS Organizations. Para obter mais informações, consulte [AWS Account Management and AWS Organizations](#) no AWS Organizations User Guide. Para obter informações gerais sobre como o acesso confiável funciona, consulte [Usando AWS Organizations com outros AWS serviços](#).

Depois que o acesso confiável tiver sido habilitado, você poderá usar o parâmetro accountID nas [operações da API de Gerenciamento de Contas](#) compatíveis. Você só poderá usar esse parâmetro

com êxito se chamar a operação usando credenciais da conta de gerenciamento ou da conta de administrador delegado da sua organização, se você habilitar uma. Para obter mais informações, consulte [Habilitar uma conta de administrador delegada para AWS Gerenciamento de contas](#).

Use o procedimento a seguir para habilitar o acesso confiável para o Gerenciamento de Contas na organização.

Permissões mínimas

Para executar essas tarefas, você deve atender aos seguintes requisitos:

- Você só pode executar essas tarefas na conta de gerenciamento da organização.
- A organização deve ter [todos os recursos habilitados](#).

Console de gerenciamento da AWS

Para habilitar o acesso confiável para AWS Gerenciamento de contas

1. Faça login no [console do AWS Organizations](#). É necessário fazer login como um usuário do IAM, assumir uma função do IAM ou fazer login como usuário root (não recomendado) na conta de gerenciamento da organização.
2. No painel de navegação, escolha Serviços.
3. Escolha Gerenciamento de Contas da AWS na lista de serviços.
4. Escolha Enable trusted access (Habilitar acesso confiável).
5. Na caixa de diálogo Habilitar acesso confiável para gerenciamento de AWS contas, digite enable para confirmá-lo e escolha Habilitar acesso confiável.

AWS CLI & SDKs

Para habilitar o acesso confiável para AWS Gerenciamento de contas

Depois de executar o comando a seguir, você pode usar as credenciais da conta de gerenciamento da organização para chamar as operações da API de Gerenciamento de Contas que usam o parâmetro `--accountId` para fazer referência às contas-membro de uma organização.

- AWS CLI: [enable-aws-service-access](#)

O exemplo a seguir permite acesso confiável para gerenciamento de AWS contas na organização da conta chamadora.

```
$ aws organizations enable-aws-service-access \
  --service-principal account.amazonaws.com
```

Se for bem-sucedido, esse comando não produzirá uma saída.

Habilitar uma conta de administrador delegada para AWS Gerenciamento de contas

Essas instruções explicam como habilitar uma conta de administrador delegado para gerenciamento de AWS contas se você se inscreveu para AWS usar o Sign up for AWS (avançado) ou se tiver ativado recursos avançados para sua conta. Para comparar as opções de inscrição, consulte [Compare as opções de inscrição](#).

Você pode registrar uma conta de administrador delegado por organização para o serviço de gerenciamento de AWS contas. Depois de registrar essa conta, os usuários e as funções dessa conta podem chamar as operações do AWS SDK AWS CLI e do SDK no account namespace que podem funcionar no modo Organizações com suporte a um parâmetro opcional. AccountId Isso permite que o administrador delegado chame as operações da API de gerenciamento de AWS contas para outras contas de membros em AWS Organizations.

Para registrar uma conta-membro na organização como conta de administrador delegado, use o procedimento a seguir.

AWS CLI & SDKs

Para registrar uma conta de administrador delegado para o serviço de Gerenciamento de Contas

Use os comandos a seguir para habilitar um administrador delegado para o serviço de Gerenciamento de Contas.

Permissões mínimas

Para executar essas tarefas, você deve atender aos seguintes requisitos:

- Você só pode executar essas tarefas na conta de gerenciamento da organização.
- A organização deve ter [todos os recursos habilitados](#).

- É preciso que tenha sido [habilitado acesso confiável para o Gerenciamento de Contas na organização](#).

Você deve especificar a seguinte entidade principal de serviço:

```
account.amazonaws.com
```

- AWS CLI: [register-delegated-administrator](#)

O exemplo a seguir registra uma conta-membro da organização como administrador delegado para o serviço de Gerenciamento de Contas.

```
$ aws organizations register-delegated-administrator \
  --account-id 123456789012 \
  --service-principal account.amazonaws.com
```

Se for bem-sucedido, esse comando não produzirá uma saída.

Depois de executar esse comando, você pode usar as credenciais da conta 123456789012 para chamar as operações de gerenciamento de contas AWS CLI e da API SDK que usam o `--account-id` parâmetro para referenciar contas membros em uma organização.

Console de gerenciamento da AWS

Essa tarefa não é suportada no console de gerenciamento de AWS contas. Você pode realizar essa tarefa somente usando a AWS CLI ou uma operação de API de um dos AWS SDKs.

Restrinja o acesso usando AWS Organizations políticas de controle de serviço

Essas informações são sobre como restringir o acesso usando políticas AWS Organizations de controle de serviço se você se inscreveu para AWS usar o Sign up for AWS (avançado) ou se tiver ativado recursos avançados para sua conta. Para comparar as opções de inscrição, consulte [Compare as opções de inscrição](#).

Este tópico apresenta exemplos que mostram como você pode usar as políticas de controle de serviços (SCPs) no AWS Organizations para restringir o que os usuários e os perfis das contas da

organização podem fazer. Para obter mais informações sobre políticas de controle de serviços, consulte os seguintes tópicos no AWS Organizations User Guide:

- [Criação de SCPs](#)
- [Como anexar SCPs a UOs e contas](#)
- [Estratégias para SCPs](#)
- [Sintaxe da política de SCP](#)

Example Exemplo 1: impedir que as contas modifiquem seus próprios contatos alternativos

O exemplo a seguir impede que as operações de API `PutAlternateContact` e `DeleteAlternateContact` sejam chamadas por qualquer conta-membro no [modo de conta autônoma](#). Isso impede que qualquer entidade principal das contas afetadas altere seus próprios contatos alternativos.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Statement1",
      "Effect": "Deny",
      "Action": [
        "account:PutAlternateContact",
        "account>DeleteAlternateContact"
      ],
      "Resource": [ "arn:aws:account::*:account" ]
    }
  ]
}
```

Example Exemplo 2: impedir que qualquer conta-membro modifique contatos alternativos para qualquer outra conta-membro da organização

O exemplo a seguir generaliza o elemento `Resource` como `"*"`, o que significa que ele se aplica tanto às [solicitações do modo autônomo quanto às solicitações do modo organizações](#). Isso significa que até mesmo a conta de administrador delegado para o Gerenciamento de Contas, se a SCP

se aplicar a ela, estará impedida de alterar qualquer contato alternativo para qualquer conta da organização.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Statement1",
      "Effect": "Deny",
      "Action": [
        "account:PutAlternateContact",
        "account>DeleteAlternateContact"
      ],
      "Resource": [ "*" ]
    }
  ]
}
```

Example Exemplo 3: impedir que uma conta-membro de uma UO modifique seus próprios contatos alternativos

O exemplo de SCP a seguir inclui uma condição que compara o caminho da organização da conta com uma lista de duas UOs. Isso resulta no bloqueio de uma entidade principal em qualquer conta das UOs especificadas para modificar seus próprios contatos alternativos.

Quando usar AWS Control Tower

Essas informações são sobre quando usar AWS Control Tower se você se inscreveu para AWS usar o Sign up for AWS (avançado) ou se tiver ativado recursos avançados para sua conta. Para comparar as opções de inscrição, consulte [Compare as opções de inscrição](#).

AWS Organizations é o serviço básico que permite gerenciar e proteger centralmente todo o AWS seu ambiente. Um componente crucial dessa abordagem AWS Organizations centrada é. AWS Control Tower AWS Control Tower atua como um console de gerenciamento nas organizações, fornecendo uma maneira simplificada de configurar e administrar um AWS ambiente seguro com várias contas, aplicando as melhores práticas prescritivas.

Essa abordagem de melhores práticas de segurança fornecida pelo AWS Control Tower amplia os principais recursos do AWS Organizations. AWS Control Tower aplica um conjunto de barreiras preventivas e de detetive para ajudar a garantir que sua organização e suas contas permaneçam alinhadas com os padrões recomendados de segurança e conformidade.

Ao estabelecer uma AWS Organizations estrutura bem arquitetada com AWS Control Tower, você pode implantar rapidamente um ambiente escalável, seguro e compatível. AWS Essa abordagem centralizada de gerenciamento e governança da nuvem é essencial para empresas que buscam aproveitar todo o poder da nuvem e, ao Nuvem AWS mesmo tempo, manter os mais altos padrões de segurança e conformidade.

Para obter mais informações, consulte [O que é o AWS Control Tower?](#) no Manual do usuário do AWS Control Tower .

Noções básicas dos modos de operação da API

Essas informações são sobre como entender os modos de operação da API se você se inscreveu para AWS usar o Sign up for AWS (avançado) ou se tiver ativado recursos avançados para sua conta. Para comparar as opções de inscrição, consulte [Compare as opções de inscrição](#).

As operações de API que funcionam com os atributos Conta da AWS de an sempre funcionam em um dos dois modos de operação:

- Contexto autônomo: esse modo é usado quando um usuário ou perfil de uma conta acessa ou altera um atributo da mesma conta. O modo de contexto independente é usado automaticamente quando você não inclui o `AccountId` parâmetro ao chamar uma das operações de gerenciamento de contas AWS CLI ou AWS SDK.
- Contexto de organizações: esse modo é usado quando um usuário ou perfil de uma conta de uma organização acessa ou altera um atributo de uma conta-membro diferente da mesma organização. O modo de contexto da organização é usado automaticamente quando você inclui o `AccountId` parâmetro ao chamar uma das operações de gerenciamento de contas AWS CLI ou AWS SDK. Você só pode chamar as operações nesse modo na conta de gerenciamento da organização ou na conta do administrador delegado para o Gerenciamento de Contas.

As operações do AWS SDK AWS CLI e do SDK podem funcionar tanto no contexto autônomo quanto no contexto organizacional.

- Se você não incluir o parâmetro `AccountId`, a operação será executada no contexto autônomo e aplicará automaticamente a solicitação à conta que você usou para fazer a solicitação. Isso é válido independentemente de a conta ser ou não membro de uma organização.
- Se você incluir o parâmetro `AccountId`, a operação será executada no contexto de organizações e funcionará na conta especificada do Organizations.
 - Se a conta que estiver chamando a operação for a conta de gerenciamento ou a conta do administrador delegado para o serviço de Gerenciamento de Contas, você poderá especificar qualquer conta-membro dessa organização no parâmetro `AccountId` para atualizar a conta especificada.
 - A única conta de uma organização que pode chamar uma das operações de contato alternativo e especificar seu próprio número de conta no parâmetro `AccountId` é a conta especificada como a [conta do administrador delegado](#) para o serviço de Gerenciamento de Contas. Qualquer outra conta, incluindo a conta de gerenciamento, recebe uma exceção `AccessDenied`.
- Se você executar uma operação no modo autônomo, deverá ter permissão para executar a operação com uma política do IAM que inclua um elemento `Resource` de qualquer "*" para permitir todos os recursos ou um [ARN que use a sintaxe para uma conta independente](#).
- Se você executar uma operação no modo de organizações, deverá ter permissão para executar a operação com uma política do IAM que inclua um elemento `Resource` de qualquer "*" para permitir todos os recursos ou um [ARN que use a sintaxe para uma conta-membro de uma organização](#).

Conceder permissões para atualizar atributos da conta

Como na maioria das AWS operações, você concede permissões para adicionar, atualizar ou excluir atributos da conta Contas da AWS usando políticas de permissão [do IAM](#). Ao anexar uma política de permissão do IAM a uma entidade principal do IAM (um usuário ou um perfil), você especifica quais ações essa entidade principal pode executar em quais recursos e sob quais condições.

A seguir são mostradas algumas considerações específicas do Gerenciamento de Contas para a criação de uma política de permissões.

Formato de nome de recurso da Amazon para Contas da AWS

- O nome de recurso da [Amazon \(ARN\)](#) para um Conta da AWS que você pode incluir no `resource` elemento de uma declaração de política é construído de forma diferente com base no fato de a conta que você deseja referenciar ser uma conta independente ou uma conta que está

em uma organização. Consulte a seção anterior em [Noções básicas dos modos de operação da API](#).

- Um ARN de conta para uma conta autônoma:

```
arn:aws:account::{AccountId}:account
```

Você deve usar esse formato quando executar uma operação de atributos de conta no modo autônomo, não incluindo o parâmetro Account ID.

- Um ARN de conta para uma conta-membro em uma organização:

```
arn:aws:account::{ManagementAccountId}:account/o-{OrganizationId}/{AccountId}
```

Você deve usar esse formato quando executar uma operação de atributos de conta em organizações, incluindo o parâmetro Account ID.

Chaves de contexto para políticas do IAM

O serviço de Gerenciamento de Contas também fornece várias [chaves de condição específicas do serviço de Gerenciamento de Contas](#) que fornecem controle refinado sobre as permissões que você concede.

conta: AccountResourceOrgPaths

A chave de contexto `account:AccountResourceOrgPaths` permite que você especifique um caminho através da hierarquia da organização para uma unidade organizacional (UO) específica. Somente as contas-membro contidas nessa UO correspondem à condição. O exemplo de trecho a seguir restringe a política para ser aplicada somente a contas que estejam em qualquer uma das duas UOs especificadas.

Como `account:AccountResourceOrgPaths` é um tipo de string multivalor, você deve usar os operadores de string de vários valores [ForAnyValue](#) ou [ForAllValues](#). Além disso, observe que o prefixo na chave de condição é `account`, mesmo que você esteja referenciando caminhos para OUs em uma organização.

```
"Condition": {
  "ForAnyValue:StringLike": {
```

```

    "account:AccountResourceOrgPaths": [
      "o-aa111bb222/r-a1b2/ou-a1b2-f6g7h111/*",
      "o-aa111bb222/r-a1b2/ou-a1b2-f6g7h222/*"
    ]
  }
}

```

conta: AccountResourceOrgTags

A chave de contexto `account:AccountResourceOrgTags` permite que você faça referência às tags que podem ser anexadas a uma conta em uma organização. Uma tag é um par de key/value strings que você pode usar para categorizar e rotular os recursos em sua conta. Para obter mais informações sobre marcação, consulte [Tag Editor](#) no Grupos de recursos da AWS User Guide. Para obter informações sobre o uso de tags como parte de uma estratégia de controle de acesso baseado em atributos, consulte [What is ABAC for AWS](#) no Guia do usuário do IAM. O exemplo de trecho seguir restringe a política para ser aplicada somente a contas de uma organização que tenham a tag com a chave `project` e um valor de `blue` ou `red`.

Como `account:AccountResourceOrgTags` é um tipo de string multivalor, você deve usar os operadores de string de vários valores [ForAnyValue](#) ou [ForAllValues](#). Além disso, observe que o prefixo na chave de condição é `account`, mesmo que você esteja fazendo referência às tags na conta de membro de uma organização.

```

"Condition": {
  "ForAnyValue:StringLike": {
    "account:AccountResourceOrgTags/project": [
      "blue",
      "red"
    ]
  }
}

```

Note

Você pode anexar tags a apenas uma conta de uma organização. Você não pode anexar tags a um aplicativo independente. Conta da AWS

Configure seu Conta da AWS

Estas instruções explicam como configurar Conta da AWS se você se inscreveu para AWS usar o Sign up for AWS (avançado) ou se ativou recursos avançados para sua conta. Para comparar as opções de inscrição, consulte [Compare as opções de inscrição](#).

Esta seção inclui tópicos que descrevem como gerenciar seu Conta da AWS.

Note

Se você Conta da AWS foi criado na Índia usando a Amazon Web Services India Private Limited (AWS Índia), há outras considerações. Para obter mais informações, consulte [Gerenciar contas na Índia](#).

Tópicos

- [Crie um Conta da AWS alias](#)
- [Ativar ou desativar Regiões da AWS na sua conta](#)
- [Atualize o faturamento do seu Conta da AWS](#)
- [Atualize o endereço de e-mail do usuário-raiz](#)
- [Atualizar senha do usuário-raiz](#)
- [Atualize seu Conta da AWS name](#)
- [Atualize os contatos alternativos para seu Conta da AWS](#)
- [Atualize o contato principal do seu Conta da AWS](#)
- [Visualizar Conta da AWS identificadores](#)

Crie um Conta da AWS alias

Essas instruções explicam como criar um Conta da AWS alias se você se inscreveu para AWS usar o Sign up for AWS (avançado) ou se tiver ativado recursos avançados para sua conta. Para comparar as opções de inscrição, consulte [Compare as opções de inscrição](#).

Se você quiser que o URL dos usuários do IAM contenha o nome da sua empresa (ou outro identificador fácil de lembrar) em vez do Conta da AWS ID, você pode criar um alias de conta.

Para saber como criar ou atualizar um alias de conta, consulte Como [usar um alias para seu Conta da AWS ID](#) no Guia do usuário do IAM.

Ativar ou desativar Regiões da AWS na sua conta

Essas informações são sobre como ativar ou desativar Regiões da AWS Conta da AWS se você se inscreveu para AWS usar o Sign up for AWS (avançado) ou se tiver ativado recursos avançados para sua conta. Para comparar as opções de inscrição, consulte [Compare as opções de inscrição](#).

An Região da AWS é um local físico no mundo com AWS várias zonas de disponibilidade. As zonas de disponibilidade consistem em um ou mais AWS data centers discretos, cada um com alimentação, rede e conectividade redundantes, alojados em instalações separadas. Isso significa que cada uma Região da AWS está fisicamente isolada e independente das outras regiões. As regiões fornecem tolerância a falhas, estabilidade e resiliência e também podem reduzir a latência. Executar cargas de trabalho em um local Região da AWS mais próximo dos usuários finais pode melhorar o desempenho e reduzir a latência. Para obter um mapa das regiões disponíveis e futuras, consulte [Regiões e zonas de disponibilidade](#). Para saber mais sobre a arquitetura Regiões da AWS de resiliência para suas cargas de trabalho, visite Fundamentos de [AWS várias regiões](#).

Regiões da AWS geralmente se enquadram em duas categorias de disponibilidade para contas:

- Regiões padrão: regiões lançadas antes de 20 de março de 2019 são habilitadas por padrão. Você pode criar e gerenciar recursos nessas regiões padrão imediatamente após a ativação da sua conta. As regiões padrão não podem ser habilitadas ou desabilitadas.
- Opt-in Regiões — As regiões lançadas após 20 de março de 2019 são desativadas por padrão e são chamadas de regiões opcionais. As regiões de aceitação desativadas não são mostradas na barra de navegação do console e você não pode usar essas regiões para criar workloads até que estejam habilitadas. Para usar essas regiões opcionais, você deve primeiro habilitá-las em seu Conta da AWS. Depois de habilitar uma região de aceitação, será possível selecionar essa região na barra de navegação e criar e gerenciar recursos nessa região. Para ativar uma região opcional para suas contas autônomas, consulte [Habilitar ou desabilitar região para contas autônomas](#) e para habilitar uma região opcional para suas contas de membros, consulte [Habilitar ou desabilitar uma região na organização](#)

Quando você se inscreve em um Conta da AWS, AWS recomenda uma região opcional para você com base no país do seu endereço de contato. Clientes em um país com uma região de AWS aceitação veem uma recomendação na página de informações de contato para ativar a região de aceitação nesse país. Clientes em um país com uma região de aceitação e uma região padrão, como

Índia, Austrália ou Canadá, recebem uma recomendação para selecionar a região de aceitação se a região de aceitação estiver mais próxima deles do que a região padrão. Depois que uma conta é ativada, você pode ativar outras regiões AWS opcionais em sua conta ou optar por desativar a região de aceitação que você ativou durante a inscrição.

Quando você cria um Conta da AWS, seus dados e credenciais do IAM são automaticamente configurados para funcionar em todas as regiões padrão, permitindo que o usuário raiz e as identidades do IAM com as permissões apropriadas acessem AWS os serviços nessas regiões usando suas credenciais existentes. AWS As regiões opt-in estão desativadas por padrão, e os dados e as credenciais do IAM não estão inicialmente disponíveis nessas regiões, o que impede o acesso aos AWS serviços nessa região. Quando você escolhe habilitar uma região de aceitação, a AWS propaga seus dados e credenciais do IAM para essa região. Depois que a propagação for concluída e a região de aceitação ativada, o usuário raiz e as identidades do IAM poderão acessar os AWS serviços na região de aceitação recém-ativada usando as mesmas credenciais do IAM que usam nas regiões padrão.

Quando você desabilita uma região de aceitação, suas credenciais do IAM são desabilitadas e você perde o acesso do IAM aos recursos dessa região. A desabilitação de uma região de aceitação não exclui os recursos dessa região e as cobranças por recursos (se houver) nessa região de aceitação desabilitada continuam sendo acumuladas na taxa padrão.

 Important

A desativação de uma região desativa o acesso do IAM aos recursos na região. Isso não exclui os recursos em questão, que continuam incorrendo em cobranças. Remova todos os recursos restantes antes de desativar uma região.

AWS agrupa regiões em [partições](#). Cada região está em exatamente uma partição, e cada partição tem uma ou mais regiões. As partições têm instâncias independentes de AWS Identity and Access Management (IAM) e fornecem um limite rígido entre regiões em diferentes partições. AWS As regiões comerciais estão na `aws` partição, as regiões na China estão na `aws-cn` partição e AWS GovCloud (US) as regiões estão na `aws-us-gov` partição. Dependendo da partição em que você criou a sua Conta da AWS, você pode usar Regiões da AWS dentro dessa partição.

- Uma conta na `aws` partição fornece acesso a várias regiões na partição comercial para que você possa lançar AWS recursos em locais que atendam às suas necessidades. Por exemplo, talvez

você queira executar instâncias do Amazon EC2 na Europa para estar mais próximo dos seus clientes europeus ou para cumprir requisitos jurídicos.

- Uma conta na aws-us-gov partição fornece acesso à região AWS GovCloud (US-West) e à região AWS GovCloud (US-East). Para obter mais informações, consulte [AWS GovCloud \(US\)](#).
- Uma conta na partição aws-cn fornece acesso somente às regiões Pequim e Ningxia. Para obter mais informações, consulte [Amazon Web Services na China](#).

Tópicos

- [Referência de disponibilidade regional](#)
- [Considerações antes de habilitar e desabilitar regiões](#)
- [Tempos de processamento e limites de solicitação](#)
- [Habilitar ou desabilitar região para contas autônomas](#)
- [Habilitar ou desabilitar uma região na organização](#)

Referência de disponibilidade regional

As tabelas a seguir listam Regiões da AWS por tipo de disponibilidade. As regiões padrão são habilitadas automaticamente e não podem ser desabilitadas, enquanto as regiões de aceitação devem ser habilitadas manualmente antes que você possa usá-las:

Opt-in Regions

As seguintes regiões são regiões de aceitação que devem ser habilitadas antes que você possa usá-las:

Nome	Código	Status
África (Cidade do Cabo)	af-south-1	GA
Ásia-Pacífico (Hong Kong)	ap-east-1	GA
Ásia-Pacífico (Taipei)	ap-east-2	GA
Ásia-Pacífico (Hyderabad)	ap-south-2	GA
Ásia-Pacífico (Jacarta)	ap-southeast-3	GA

Nome	Código	Status
Ásia-Pacífico (Melbourne)	ap-southeast-4	GA
Ásia-Pacífico (Malásia)	ap-southeast-5	GA
Ásia-Pacífico (Nova Zelândia)	ap-southeast-6	GA
Ásia-Pacífico (Tailândia)	ap-southeast-7	GA
Oeste do Canadá (Calgary)	ca-west-1	GA
Europa (Zurique)	eu-central-2	GA
Europa (Milão)	eu-south-1	GA
Europa (Espanha)	eu-south-2	GA
Israel (Tel Aviv)	il-central-1	GA
Oriente Médio (Emirados Árabes Unidos)	me-central-1	GA
Oriente Médio (Bahrein)	me-south-1	GA
México (Centro)	mx-central-1	GA

Default Regions

As seguintes regiões estão habilitadas por padrão e não podem ser desabilitadas:

Nome	Código
Ásia-Pacífico (Tóquio)	ap-northeast-1
Ásia-Pacífico (Seul)	ap-northeast-2
Asia Pacific (Osaka)	ap-northeast-3
Ásia-Pacífico (Mumbai)	ap-south-1

Nome	Código
Ásia-Pacífico (Singapura)	ap-southeast-1
Ásia-Pacífico (Sydney)	ap-southeast-2
Canadá (Central)	ca-central-1
Europa (Frankfurt)	eu-central-1
Europa (Estocolmo)	eu-north-1
Europa (Irlanda)	eu-west-1
Europa (Londres)	eu-west-2
Europa (Paris)	eu-west-3
América do Sul (São Paulo)	sa-east-1
Leste dos EUA (Norte da Virgínia)	us-east-1
Leste dos EUA (Ohio)	us-east-2
Oeste dos EUA (N. da Califórnia)	us-west-1
Oeste dos EUA (Oregon)	us-west-2

Para obter uma lista de nomes de região e seus respectivos códigos, consulte [Regional endpoints](#) no AWS General Reference Guide. Para obter uma lista dos AWS serviços suportados em cada região (sem endpoints), consulte a Lista [de serviços](#) AWS regionais.

Important

AWS recomenda que você use endpoints regionais AWS Security Token Service (AWS STS) em vez do endpoint global para reduzir a latência. Os tokens de sessão dos AWS STS endpoints regionais são válidos em todas as AWS regiões. Se você usa AWS STS endpoints regionais, não precisa fazer nenhuma alteração. No entanto, os tokens de sessão do AWS STS endpoint global (<https://sts.amazonaws.com>) são válidos somente Regiões da AWS se você habilitar ou se estiverem habilitados por padrão. Se você pretende habilitar uma nova

região para sua conta, você pode usar tokens de sessão de AWS STS endpoints regionais ou ativar o AWS STS endpoint global para emitir tokens de sessão que sejam válidos em todos. Regiões da AWS Tokens de sessão válidos em todas as regiões são maiores. Se você armazenar tokens de sessão, esses tokens maiores podem afetar seus sistemas. Para obter mais informações sobre como AWS STS os endpoints funcionam com AWS regiões, consulte [Gerenciando AWS STS em uma AWS região](#).

Considerações antes de habilitar e desabilitar regiões

Antes de habilitar ou desabilitar uma região, é importante considerar o seguinte:

- Você pode usar todas as regiões de destino em uma geografia de inferência entre regiões, independentemente do Region-opt status — Alguns serviços AWS generativos de IA, incluindo Amazon Bedrock (consulte [Aumentar a taxa de transferência com inferência entre regiões](#)) e Amazon Q Developer (veja [Cross-region processamento no Amazon Q Developer](#)) usam [inferência entre regiões](#). Se você usa esses serviços, eles selecionam automaticamente a Região da AWS ideal, incluindo as regiões que você não habilitou para recursos e dados do IAM, dentro da geografia escolhida. Isso melhora a experiência do cliente ao maximizar a disponibilidade da computação e do modelo disponível.
- Você pode usar as permissões do IAM para controlar o acesso às regiões — AWS Identity and Access Management (IAM) inclui quatro permissões que permitem controlar quais usuários podem ativar, desativar, obter e listar regiões. Para obter mais informações, consulte [AWS: permite habilitar e desabilitar Regiões da AWS](#) no Guia do usuário do IAM. Você também pode usar a chave de [aws:RequestedRegion](#) condição para controlar o acesso Serviços da AWS a um Região da AWS.
- Habilitar e desabilitar uma região é grátis: a habilitação e desabilitação de uma região não é cobrada. Você é cobrado somente pelos recursos criados na nova região.
- EventBridge Integração com a Amazon — Você pode se inscrever para receber notificações de atualização de status de opção regional em. EventBridge Uma EventBridge notificação será criada para cada alteração de status, permitindo que os clientes automatizem os fluxos de trabalho.
- Region-opt Status expressivo — Devido à natureza assíncrona de enabling/disabling uma região de aceitação, há quatro possíveis status para uma solicitação de aceitação por região:
 - ENABLING
 - DISABLING
 - ENABLED

- DISABLED

Você não pode cancelar uma operação de ativação ou desativação que esteja no status `ENABLING` ou `DISABLING`. Caso contrário, uma `ConflictException` será lançada. Uma solicitação de opção por região concluída (`Enabled/Disabled`) depende do provisionamento dos principais serviços subjacentes. AWS pode haver alguns AWS serviços que não possam ser usados imediatamente, apesar do status ser `ENABLED`.

Tempos de processamento e limites de solicitação

Ao habilitar ou desabilitar regiões, esteja ciente das seguintes limitações de tempo e solicitação:

- A operação de habilitar uma região leva de alguns minutos a várias horas, em alguns casos: quando você habilita uma região, a AWS executa ações para preparar a conta nesta região, como a distribuição dos recursos do IAM para a região. Esse processo leva alguns minutos para a maioria das contas, mas pode, às vezes, levar várias horas. Você não pode usar a região até que esse processo seja concluído.
- Desabilitar uma região nem sempre é algo imediatamente visível: os serviços e os consoles podem ficar temporariamente visíveis depois que uma região é desabilitada. A desativação de uma região pode levar de alguns minutos a várias horas para entrar em vigor.
- Uma única conta pode ter seis solicitações de opção de ativação ou desativação de regiões em andamento a qualquer momento: uma solicitação equivale a habilitar ou desabilitar uma região específica para uma conta.
- As organizações podem ter 50 solicitações de opção regional abertas em um determinado momento em toda a AWS organização — A conta de gerenciamento pode, a qualquer momento, ter 50 solicitações abertas pendentes de conclusão para sua organização. Uma solicitação equivale a habilitar ou desabilitar uma região específica para uma conta.

Habilitar ou desabilitar região para contas autônomas

Para atualizar as regiões às quais você Conta da AWS tem acesso, execute as etapas do procedimento a seguir. O Console de gerenciamento da AWS procedimento a seguir sempre funciona somente no contexto autônomo. Você pode usar o Console de gerenciamento da AWS para visualizar ou atualizar somente as regiões disponíveis na conta usada para chamar a operação.

Console de gerenciamento da AWS

Para habilitar ou desabilitar uma região para um autônomo Conta da AWS

Permissões mínimas

Para executar as etapas do procedimento a seguir, um usuário ou perfil do IAM deve ter as seguintes permissões:

- `account:ListRegions`(necessário para ver a lista Regiões da AWS e se eles estão atualmente ativados ou desativados).
- `account:EnableRegion`
- `account:DisableRegion`

1. Faça login no [Console de gerenciamento da AWS](#) como ou como um usuário Usuário raiz da conta da AWS ou função do IAM que tenha as permissões mínimas.
2. Escolha o nome da conta no canto superior direito da janela e depois escolha Conta.
3. Na página [Conta](#), role para baixo até a seção Regiões da AWS.
4. Escolha a região que você deseja habilitar e desabilitar e escolha a ação desejada Habilitar ou Desabilitar. Você verá um prompt para confirmar.
5. Se você tiver escolhido a opção Habilitar, analise o texto exibido e escolha Habilitar região.

Se você tiver escolhido a opção Desabilitar, analise o texto exibido, digite **disable** para confirmar e escolha Desabilitar região.

Depois que a região de aceitação for habilitada, você poderá selecionar essa região na barra de navegação da região. Para as etapas de seleção de uma região, consulte [Escolher uma região pela barra de navegação no Console de gerenciamento da AWS](#) e para a configuração específica do console da região em sua conta, consulte [Definir a região padrão no Console de gerenciamento da AWS](#).

AWS CLI & SDKs

Você pode ativar, desativar, ler e listar o status de opção da região usando os seguintes AWS CLI comandos ou suas operações equivalentes no AWS SDK:

- `EnableRegion`

- `DisableRegion`
- `GetRegionOptStatus`
- `ListRegions`

Permissões mínimas

Para executar as etapas a seguir, é necessário ter a permissão que é mapeada para essa operação:

- `account:EnableRegion`
- `account:DisableRegion`
- `account:GetRegionOptStatus`
- `account:ListRegions`

Se você usar essas permissões individuais, poderá conceder a alguns usuários a capacidade de ler somente as informações de opção de ativação e desativação da região e conceder a outros a capacidade de ler e gravar.

O exemplo a seguir habilita uma região para a conta-membro especificada em uma organização. As credenciais usadas devem pertencer à conta de gerenciamento da organização ou à conta de administrador delegado do serviço de Gerenciamento de Contas.

Você também pode desabilitar uma região usando o mesmo comando e, depois, substituindo `enable-region` por `disable-region`.

```
aws account enable-region --region-name af-south-1
```

Se for bem-sucedido, esse comando não produzirá uma saída.

A operação é assíncrona. O comando a seguir permitirá que você veja o status mais recente da solicitação.

```
aws account get-region-opt-status --region-name af-south-1
{
  "RegionName": "af-south-1",
  "RegionOptStatus": "ENABLING"
}
```

Habilitar ou desabilitar uma região na organização

Para atualizar as regiões habilitadas para suas contas de membros AWS Organizations, execute as etapas do procedimento a seguir.

Note

As políticas AWS Organizations `AWSOrganizationsReadOnlyAccess` gerenciadas `AWSOrganizationsFullAccess` são atualizadas para fornecer permissão para acessar as APIs de gerenciamento de AWS contas para que você possa acessar os dados da conta no AWS Organizations console. Para ver as políticas gerenciadas atualizadas, consulte [Atualizações nas políticas AWS gerenciadas das organizações](#).

Note

Antes de executar essas operações na conta de gerenciamento ou em uma conta de administrador delegado em uma organização para uso com contas-membro, você deve:

- Habilitar todos os recursos na sua organização para gerenciar as configurações das contas-membro. Isso permite o controle administrativo das contas-membro. Isso é definido por padrão quando você cria sua organização. Se sua organização estiver configurada somente para faturamento consolidado e você quiser habilitar todos os recursos, consulte [Enabling all features in your organization](#).
- Habilite o acesso confiável para o serviço de gerenciamento de AWS contas. Para configurar isso, consulte [Habilite o acesso confiável para AWS Gerenciamento de contas](#).

Console de gerenciamento da AWS

Para habilitar ou desabilitar uma região na organização

1. Faça login no AWS Organizations console com as credenciais da conta de gerenciamento da sua organização.
2. Na página Contas da AWS, selecione a conta que você deseja atualizar.
3. Selecione a guia Configurações da conta.
4. Em Regiões, selecione a região que você deseja habilitar ou desabilitar.

5. Escolha Ações e, em seguida, escolha a opção Habilitar ou Desabilitar.
6. Se você tiver escolhido a opção Habilitar, analise o texto exibido e escolha Habilitar região.
7. Se você tiver escolhido a opção Desabilitar, analise o texto exibido, digite desabilitar para confirmar e, em seguida, escolha Desabilitar região.

AWS CLI & SDKs

Você pode ativar, desativar, ler e listar o status de opção de região para contas de membros da organização usando os seguintes AWS CLI comandos ou suas operações equivalentes no AWS SDK:

- `EnableRegion`
- `DisableRegion`
- `GetRegionOptStatus`
- `ListRegions`

Permissões mínimas

Para executar as etapas a seguir, é necessário ter a permissão que é mapeada para essa operação:

- `account:EnableRegion`
- `account:DisableRegion`
- `account:GetRegionOptStatus`
- `account:ListRegions`

Se você usar essas permissões individuais, poderá conceder a alguns usuários a capacidade de ler somente as informações de opção de ativação e desativação da região e conceder a outros a capacidade de ler e gravar.

O exemplo a seguir habilita uma região para a conta-membro especificada em uma organização. As credenciais usadas devem pertencer à conta de gerenciamento da organização ou à conta de administrador delegado do serviço de Gerenciamento de Contas.

Você também pode desabilitar uma região usando o mesmo comando e, depois, substituindo `enable-region` por `disable-region`.

```
aws account enable-region --account-id 123456789012 --region-name af-south-1
```

Se for bem-sucedido, esse comando não produzirá uma saída.

 Note

Uma organização só pode ter até 20 solicitações de região em um determinado momento. Caso contrário, você receberá uma `TooManyRequestsException`.

A operação é assíncrona. O comando a seguir permitirá que você veja o status mais recente da solicitação.

```
aws account get-region-opt-status --account-id 123456789012 --region-name af-south-1
{
  "RegionName": "af-south-1",
  "RegionOptStatus": "ENABLING"
}
```

Atualize o faturamento do seu Conta da AWS

Essas instruções são sobre como atualizar o faturamento Conta da AWS se você se inscreveu para AWS usar o Sign up for AWS (avançado) ou se tiver ativado recursos avançados para sua conta. Para comparar as opções de inscrição, consulte [Compare as opções de inscrição](#).

Você pode atualizar todas as suas preferências de Conta da AWS cobrança usando o console AWS Billing de gerenciamento de custos. Para saber como atualizar as configurações relacionadas ao faturamento da conta, consulte o [Guia do usuário do Gerenciamento de Faturamento e Custos da AWS](#):

Atualize o endereço de e-mail do usuário-raiz

Essas instruções são sobre como atualizar o endereço de e-mail do usuário root se você se inscreveu para AWS usar o Sign up for AWS (avançado) ou se tiver ativado recursos avançados para sua conta. Para comparar as opções de inscrição, consulte [Compare as opções de inscrição](#).

Há vários motivos comerciais pelos quais você pode precisar atualizar o endereço de e-mail do usuário-raiz para sua Conta da AWS. Por exemplo, segurança e resiliência administrativa. Este tópico explica o processo de atualização do endereço de e-mail do usuário-raiz para contas autônomas e de membros.

 Note

As alterações em um Conta da AWS podem levar até quatro horas para se propagar em todos os lugares.

Você pode atualizar o e-mail do usuário-raiz de forma diferente, dependendo se as contas são autônomas ou fazem parte de uma organização:

- **Contas autônomas Contas da AWS ou de gerenciamento** — Para Contas da AWS não associadas a uma organização, ou para a conta de gerenciamento de uma organização, você pode atualizar o e-mail do usuário raiz usando o AWS Management Console. Para saber como fazer isso, consulte [Atualizar o e-mail do usuário root do para uma conta autônoma Conta da AWS ou de gerenciamento](#).
- **Contas da AWS dentro de uma organização** — Para contas membros que fazem parte de uma AWS organização, um usuário na conta de gerenciamento ou na conta de administrador delegado pode atualizar centralmente o e-mail do usuário raiz conta membro a partir do AWS Organizations console ou programaticamente por meio da CLI AWS e SDKs. Para saber como fazer isso, consulte [Atualizar o e-mail do usuário raiz para qualquer pessoa Conta da AWS em sua organização](#).

Tópicos

- [Atualize o e-mail do usuário root para um autônomo Conta da AWS ou conta de gerenciamento](#)
- [Atualize o e-mail do usuário root para qualquer Conta da AWS na sua organização](#)

Atualize o e-mail do usuário root para um autônomo Conta da AWS ou conta de gerenciamento

Para editar o endereço de e-mail do usuário raiz (endereço de) para uma conta autônoma Conta da AWS ou de gerenciamento, execute as etapas no procedimento a seguir.

Console de gerenciamento da AWS

Note

Você deve fazer login como o Usuário raiz da conta da AWS, o que não requer permissões adicionais do IAM. Não é possível executar essas etapas como usuário ou perfil do IAM.

1. Use seu endereço Conta da AWS de e-mail e senha para fazer login no [Console de gerenciamento da AWS](#) como seu Usuário raiz da conta da AWS.
2. No canto superior direito do console, selecione o nome ou número de sua conta e, em seguida, selecione Conta.
3. Na página [Account](#), ao lado de Account details, escolha Actions e selecione Update email address and password.
4. Na página Account Details, ao lado de Email address, escolha Edit.
5. Na página Edit Account Email, preencha os campos New email address, Confirm new email address e confirme sua Password atual. Após, escolha Save and continue. Um código de verificação é enviado para o novo endereço de e-mail, de no-reply@verify.signin.aws.
6. Na página Edit Account Email, em Verification code, insira o código que você recebeu em seu e-mail e escolha Confirm updates.

Note

Pode levar até cinco minutos para que o código de verificação chegue. Se você não vir a mensagem na caixa de entrada, verifique as pastas de spam e lixo eletrônico.

AWS CLI & SDKs

Essa tarefa não é compatível com AWS CLI ou por uma operação de API de um dos AWS SDKs. Você pode executar essa tarefa somente usando Console de gerenciamento da AWS o.

Atualize o e-mail do usuário root para qualquer Conta da AWS na sua organização

Para editar o endereço de e-mail do usuário raiz (endereço de) de qualquer conta membro em sua organização usando o AWS Organizations console, execute as etapas no procedimento a seguir.

Note

Antes de atualizar o endereço de e-mail do usuário-raiz para uma conta de membro, recomendamos que você entenda o impacto dessa operação. Para obter mais informações, consulte [Updating the root user email address para uma conta de membro da AWS Organizations](#) no Guia do usuário do AWS Organizations .

Você também pode atualizar o endereço de e-mail do usuário raiz () de uma [conta membro diretamente da página Conta](#) Console de gerenciamento da AWS após o login como usuário raiz. Para obter instruções detalhadas, siga as etapas fornecidas em [Atualize o e-mail do usuário root para um autônomo Conta da AWS ou conta de gerenciamento](#).

Note

Você não pode atualizar o endereço de e-mail do usuário raiz de uma conta do projeto, que é uma conta de membro que você criou como um projeto nas AWS Configurações. Uma ID do AWS Builder é proprietária de cada conta do projeto em vez do endereço de e-mail do usuário raiz, e isso não muda quando você ativa os recursos avançados. Para obter mais informações, consulte [Contas do projeto depois de ativar os recursos avançados](#).

AWS Management Console

Observações

- Para realizar este procedimento com a conta de gerenciamento ou em uma conta de administrador delegado em uma organização em relação a contas-membro, você precisa [habilitar o acesso confiável ao serviço Gerenciamento de conta](#).
- Você não pode usar esse procedimento para acessar uma conta em uma organização diferente daquela que você está usando para chamar a operação.

Para atualizar o endereço de e-mail do usuário-raiz para uma conta de membro usando o AWS Organizations console

1. Faça login no [console do AWS Organizations](#). Você deve fazer login como um usuário do IAM ou fazer login como usuário-raiz ([não recomendado](#)) na conta gerencial da organização.
2. Na página Contas da AWS, escolha a conta de membro para a qual você deseja atualizar o endereço de e-mail do usuário-raiz.
3. Na seção Detalhes da conta, escolha o botão Ações e escolha Atualizar endereço de e-mail.
4. Em E-mail, insira o novo endereço de e-mail do usuário-raiz e escolha Salvar. Isso envia uma senha de uso único (OTP) para o novo endereço de e-mail.

 Note

Se precisar fechar esta página no console do Organizations enquanto espera pelo código, você pode retornar e concluir o processo de OTP dentro de 24 horas a partir do momento em que o código foi enviado. Para fazer isso, na página Detalhes da conta, escolha o botão Ações e, em seguida, escolha Concluir atualização por e-mail.

5. Em Código de verificação, insira o código que foi enviado para o novo endereço de e-mail na etapa anterior e escolha Confirmar. Isso confirma a atualização do usuário-raiz para a conta.

AWS CLI & SDKs

Você pode recuperar ou atualizar o endereço de e-mail do usuário raiz (também chamado de endereço de e-mail principal) usando os seguintes AWS CLI comandos ou suas operações equivalentes no AWS SDK:

- [GetPrimaryEmail](#)
- [StartPrimaryEmailUpdate](#)
- [AcceptPrimaryEmailUpdate](#)

 Observações

- Para executar realizar essas operações na conta de gerenciamento ou em uma conta de administrador delegado em uma organização em relação a contas-membro, você precisa [habilitar o acesso confiável ao serviço de Gerenciamento de conta](#).

- Você não pode acessar uma conta em uma organização diferente daquela que você está usando para chamar a operação.
- Para uma conta de projeto `StartPrimaryEmailUpdate` e `AcceptPrimaryEmailUpdate` falhe com um `AccessDeniedException` erro mesmo quando você tem as permissões necessárias.

Permissões mínimas

Para cada operação, você deve ter a permissão que mapeia para essa operação:

- `account:GetPrimaryEmail`
- `account:StartPrimaryEmailUpdate`
- `account:AcceptPrimaryEmailUpdate`

Se você usar essas permissões individuais, poderá conceder a alguns usuários a capacidade de ler somente as informações do endereço de e-mail do usuário-raiz e conceder a outros a capacidade de ler e gravar.

Para concluir o processo de endereço de e-mail do usuário raiz , você deve usar as APIs de e-mail primárias em conjunto na ordem em que são mostradas nos exemplos a seguir.

Example **GetPrimaryEmail**

O exemplo a seguir recupera o endereço de e-mail do usuário-raiz da conta de membro especificada em uma organização. As credenciais usadas devem pertencer à conta de gerenciamento da organização ou à conta de administrador delegado do serviço de Gerenciamento de Contas.

```
$ aws account get-primary-email --account-id 123456789012
```

Example **StartPrimaryEmailUpdate**

O exemplo a seguir inicia o processo de atualização do endereço de e-mail do usuário-raiz, identifica o novo endereço de e-mail e envia uma senha de uso único (OTP) para o novo endereço de e-mail da conta de membro especificada em uma organização. As credenciais

usadas devem pertencer à conta de gerenciamento da organização ou à conta de administrador delegado do serviço de Gerenciamento de Contas.

```
$ aws account start-primary-email-update --account-id 123456789012 --primary-email john@examplecorp.com
```

Example **AcceptPrimaryEmailUpdate**

O exemplo a seguir aceita o código OTP e define o novo endereço de e-mail para a conta-membro especificada em uma organização. As credenciais usadas devem pertencer à conta de gerenciamento da organização ou à conta de administrador delegado do serviço de Gerenciamento de Contas.

```
$ aws account accept-primary-email-update --account-id 123456789012 --otp 12345678 --primary-email john@examplecorp.com
```

Atualizar senha do usuário-raiz

Essas instruções explicam como atualizar a senha do usuário root se você se inscreveu para AWS usar o Sign up for AWS (avançado) ou se tiver ativado recursos avançados para sua conta. Para comparar as opções de inscrição, consulte [Compare as opções de inscrição](#).

Para editar sua senha Conta da AWS de usuário root, execute as etapas do procedimento a seguir.

Console de gerenciamento da AWS

Como editar sua senha de usuário-raiz

Note

Você deve fazer login como o Usuário raiz da conta da AWS, o que não requer permissões adicionais do IAM. Não é possível executar essas etapas como usuário ou perfil do IAM.

1. Use seu endereço Conta da AWS de e-mail e senha para fazer login no [Console de gerenciamento da AWS](#) como seu Usuário raiz da conta da AWS.
2. No canto superior direito do console, selecione o nome ou número de sua conta e, em seguida, selecione Conta.

3. Na página [Account](#), ao lado de Account details, escolha Actions e selecione Update email address and password.
4. Na página Account Details, ao lado de Password, escolha Edit.
5. Na página Edit password, preencha os campos Current password, New password e Confirm new password. Em seguida, selecione Update password. Para obter orientações adicionais, incluindo práticas recomendadas para definir senhas de usuário-raiz, consulte [Alterar a senha para o Usuário raiz da conta da AWS](#) no Guia do usuário do IAM.

AWS CLI & SDKs

Essa tarefa não é suportada AWS CLI nem por uma operação de API de um dos AWS SDKs. Você pode executar essa tarefa somente usando Console de gerenciamento da AWS o.

Atualize seu Conta da AWS name

Essas instruções explicam como atualizar seu Conta da AWS nome se você se inscreveu para AWS usar o Sign up for AWS (avançado) ou se tiver ativado recursos avançados para sua conta. Para comparar as opções de inscrição, consulte [Compare as opções de inscrição](#).

Ao gerenciar várias Contas da AWS, use convenções de nomenclatura claras alinhadas com unidades de negócios e aplicativos para identificação e organização. Durante reorganizações, fusões, aquisições ou atualizações de convenções de nomenclatura, talvez seja necessário renomear contas para manter padrões administrativos e de identificação consistentes.

O nome de uma conta aparece em vários lugares, como na sua fatura e em consoles, como o painel Gerenciamento de Cobrança e Custos e o console. AWS Organizations Recomendamos que você use uma forma padrão de dar nome às contas para poder dar nomes fáceis de reconhecer. Em contas corporativas, considere usar um padrão de nomenclatura, como organização-finalidade-ambiente (por exemplo, catálogo-de vendas-de produtos). Por motivos de privacidade e segurança, evite usar nomes de conta que reflitam informações de identificação pessoal (PII).

- Contas autônomas Contas da AWS ou gerenciais — Para contas Contas da AWS não associadas a uma organização ou para a conta de gerenciamento de uma organização, você pode atualizar o nome da sua conta usando os SDKs Console de gerenciamento da AWS, ou AWS CLI e. Para aprender a fazer isso, consulte [Atualize o nome da sua conta para uma conta independente Conta da AWS ou conta de gerenciamento](#).

- Contas da AWS dentro de uma organização — Para contas de membros que fazem parte de uma AWS Organizations, um usuário na conta de gerenciamento ou na conta de administrador delegado pode atualizar centralmente o nome da conta de qualquer conta membro na organização a partir do AWS Organizations console ou programaticamente por meio dos SDKs e. AWS CLI Para aprender a fazer isso, consulte [Atualize o nome da sua conta para qualquer Conta da AWS na sua organização](#).

Note

As alterações em um Conta da AWS podem levar até quatro horas para se propagarem em todos os lugares.

Tópicos

- [Atualize o nome da sua conta para uma conta independente Conta da AWS ou conta de gerenciamento](#)
- [Atualize o nome da sua conta para qualquer Conta da AWS na sua organização](#)

Atualize o nome da sua conta para uma conta independente Conta da AWS ou conta de gerenciamento

Para alterar o nome da conta de uma conta autônoma Conta da AWS ou de gerenciamento, execute as etapas do procedimento a seguir.

Console de gerenciamento da AWS

Permissões mínimas

Você pode atualizar o nome da conta usando o usuário-raiz, um usuário do IAM ou um perfil do IAM. Se você estiver usando o usuário root, nenhuma permissão adicional do IAM será necessária para atualizar o nome de uma conta. Ao usar um usuário ou perfil do IAM, você deve ter pelo menos as seguintes permissões do IAM:

- `account:GetAccountInformation`
- `account:PutAccountName`

Para atualizar o nome da conta de uma conta autônoma ou de gerenciamento

1. Use seu endereço Conta da AWS de e-mail e senha para fazer login no [Console de gerenciamento da AWS](#) como seu Usuário raiz da conta da AWS.
2. No canto superior direito do console, selecione o nome ou número de sua conta e, em seguida, selecione Conta.
3. Na página [Conta](#), ao lado de Detalhes da conta, escolha Ações e selecione Atualizar nome da conta.
4. Em Nome, insira o novo nome da conta que você deseja atualizar e escolha Salvar.

AWS CLI & SDKs

Permissões mínimas

Você pode atualizar o nome da conta usando o usuário-raiz, um usuário do IAM ou um perfil do IAM. Para executar as etapas a seguir, seu usuário ou perfil do IAM deve ter, no mínimo, as seguintes permissões do IAM:

- `account:GetAccountInformation`
- `account:PutAccountName`

Para atualizar o nome da conta de uma conta autônoma ou de gerenciamento

Você também pode usar as seguintes operações:

- AWS CLI: [put-account-name](#)

```
$ C:\> aws account put-account-name \
    --account-name "New-Account-Name"
```

- AWS SDKs: [PutAccountName](#)

Atualize o nome da sua conta para qualquer Conta da AWS na sua organização

No modo AWS Organizations com todos os recursos, usuários autorizados do IAM ou funções do IAM nas contas de gerenciamento e de administração delegada podem gerenciar centralmente os nomes das contas.

Para alterar o nome da conta de uma conta de membro de uma organização, execute as etapas mostradas no procedimento a seguir.

Requisitos

Para atualizar o nome de uma conta com o AWS Organizations console, você precisa fazer algumas configurações preliminares:

- A organização precisa habilitar todos os atributos para gerenciar as configurações das contas de membros. Isso permite o controle administrativo das contas-membro. Isso é definido por padrão quando você cria sua organização. Se sua organização estiver configurada somente para faturamento consolidado e você quiser habilitar todos os atributos, consulte [Enabling all features for an organization](#).
- Você precisa habilitar o acesso confiável ao serviço de gerenciamento de AWS contas. Para configurar isso, consulte [Habilite o acesso confiável para AWS Gerenciamento de contas](#).

Console de gerenciamento da AWS



Permissões mínimas

Para atualizar o nome da conta de uma conta de membro, seu usuário ou perfil do IAM deve ter as seguintes permissões:

- `organizations:DescribeOrganization` (somente console)
- `account:PutAccountName`

Para atualizar o nome da conta de uma conta de membro

1. Abra o console Organizations em <https://console.aws.amazon.com/organizations/>.
2. No painel de navegação principal, escolha Contas da AWS.
3. Na página Contas da AWS, escolha a conta de membro que você deseja atualizar, escolha o menu suspenso Ações e escolha Atualizar nome da conta.

4. Em Nome, insira o nome atualizado e escolha Salvar.

AWS CLI & SDKs

Permissões mínimas

Para atualizar o nome da conta de uma conta de membro, seu usuário ou perfil do IAM deve ter as seguintes permissões:

- `organizations:DescribeOrganization` (somente console)
- `account:PutAccountName`

Para atualizar o nome da conta de uma conta de membro

Você também pode usar as seguintes operações:

- AWS CLI: [put-account-name](#)

```
$ C:\> aws account put-account-name \  
      --account-id 111111111111 \  
      --account-name "New-Account-Name"
```

- AWS SDKs: [PutAccountName](#)

Atualize os contatos alternativos para seu Conta da AWS

Essas instruções explicam como atualizar os contatos alternativos Conta da AWS se você se inscreveu para AWS usar o Sign up for AWS (avançado) ou se tiver ativado recursos avançados para sua conta. Para comparar as opções de inscrição, consulte [Compare as opções de inscrição](#).

Contatos alternativos AWS permitem contatar até três contatos alternativos associados à conta. Um contato alternativo não precisa ser uma pessoa específica. Em vez disso, você pode adicionar uma lista de distribuição de e-mail se tiver uma equipe que gerencia questões relacionadas a cobrança, operações e segurança. Eles são adicionais ao endereço de e-mail associado ao [usuário-raiz](#) da conta. O [contato principal da conta](#) continuará a receber todas as comunicações por e-mail enviadas para o e-mail da conta raiz.

Você pode especificar somente um de cada um dos tipos de contato a seguir associados a uma conta.

- Contato de faturamento
- Contato de operações
- Contato de segurança

Você pode adicionar ou editar contatos alternativos de forma diferente, dependendo se as contas são autônomas ou fazem parte de uma organização:

- Autônomo Contas da AWS — Se Contas da AWS não estiver associado a uma organização, você pode atualizar seus próprios contatos alternativos usando o AWS Management Console ou via AWS CLI e SDKs. Para saber como fazer isso, consulte [Update the alternate contacts for a standalone Conta da AWS](#).
- Contas da AWS dentro de uma organização — Para contas de membros que fazem parte de uma AWS organização, um usuário na conta de gerenciamento ou na conta de administrador delegado pode atualizar centralmente qualquer conta membro na organização a partir do AWS Organizations console ou programaticamente por meio da CLI e dos AWS SDKs. Para saber como fazer isso, consulte [Atualizar os contatos alternativos para qualquer um Conta da AWS em sua organização](#).

Tópicos

- [Requisitos de número de telefone e endereço de e-mail](#)
- [Atualize os contatos alternativos para um autônomo Conta da AWS](#)
- [Atualize os contatos alternativos para qualquer Conta da AWS na sua organização](#)
- [conta: chave de AlternateContactTypes contexto](#)

Requisitos de número de telefone e endereço de e-mail

Antes de prosseguir com a atualização das informações dos contatos alternativos da conta, recomendamos que você primeiro analise os requisitos a seguir quando inserir números de telefone e endereços de e-mail.

- Os números de telefone só podem conter números, espaços em branco e os seguintes caracteres: “+ - ()”.

- Os endereços de e-mail podem ter até 254 caracteres e podem incluir os seguintes caracteres especiais na parte local do endereço de e-mail, além dos caracteres alfanuméricos padrão: “+=. # | ! & - _”.

Atualize os contatos alternativos para um autônomo Conta da AWS

Para adicionar ou editar os contatos alternativos para um autônomo Conta da AWS, execute as etapas do procedimento a seguir. O Console de gerenciamento da AWS procedimento a seguir sempre funciona somente no contexto autônomo. Você pode usar o Console de gerenciamento da AWS para acessar ou alterar somente os contatos alternativos na conta usada para chamar a operação.

Console de gerenciamento da AWS

Para adicionar ou editar os contatos alternativos para um ambiente autônomo Conta da AWS

Permissões mínimas

Para executar as etapas a seguir, é necessário ter as seguintes permissões do IAM:

- `account:GetAlternateContact` (para ver os detalhes dos contatos alternativos)
- `account:PutAlternateContact` (para definir ou atualizar um contato alternativo)
- `account>DeleteAlternateContact` (para excluir um contato alternativo)

1. Faça login no [Console de gerenciamento da AWS](#) como um usuário ou perfil do IAM que tenha as permissões mínimas.
2. Escolha o nome da conta no canto superior direito da janela e depois escolha Conta.
3. Na página [Conta](#), role para baixo até Contatos alternativos e, à direita do título, escolha Editar.

 Note

Se você não vê a opção **Editar**, é provável que você não esteja conectado como usuário root da sua conta ou como alguém que tenha as permissões mínimas especificadas anteriormente.

4. Altere os valores em qualquer um dos campos disponíveis.

 Important

Para empresas Contas da AWS, é uma prática recomendada inserir um número de telefone e endereço de e-mail da empresa em vez de um pertencente a um indivíduo.

5. Depois de fazer todas as alterações, escolha **Atualizar**.

AWS CLI & SDKs

Você pode recuperar, atualizar ou excluir as informações de contato alternativas usando os seguintes AWS CLI comandos ou suas operações equivalentes no AWS SDK:

- [GetAlternateContact](#)
- [PutAlternateContact](#)
- [DeleteAlternateContact](#)

 Observações

- Para executar realizar essas operações na conta de gerenciamento ou em uma conta de administrador delegado em uma organização em relação a contas-membro, você precisa [habilitar o acesso confiável ao serviço Conta](#).

 Permissões mínimas

Para cada operação, você deve ter a permissão que mapeia para essa operação:

- `GetAlternateContact` (para ver os detalhes dos contatos alternativos)

- `PutAlternateContact` (para definir ou atualizar um contato alternativo)
- `DeleteAlternateContact` (para excluir um contato alternativo)

Se você usar essas permissões individuais, poderá conceder a alguns usuários a capacidade de ler somente as informações de contato e conceder a outros a capacidade de ler e gravar.

Example

O exemplo a seguir recupera o contato alternativo atual de faturamento da conta do chamador.

```
$ aws account get-alternate-contact \
  --alternate-contact-type=BILLING
{
  "AlternateContact": {
    "AlternateContactType": "BILLING",
    "EmailAddress": "saanvi.sarkar@amazon.com",
    "Name": "Saanvi Sarkar",
    "PhoneNumber": "+1(206)555-0123",
    "Title": "CF0"
  }
}
```

Example

O exemplo a seguir define um novo contato alternativo de operações da conta do chamador.

```
$ aws account put-alternate-contact \
  --alternate-contact-type=OPERATIONS \
  --email-address=mateo_jackson@amazon.com \
  --name="Mateo Jackson" \
  --phone-number="+1(206)555-1234" \
  --title="Operations Manager"
```

Se for bem-sucedido, esse comando não produzirá uma saída.

Example

Note

Se você realizar várias `PutAlternateContact` operações no mesmo Conta da AWS e no mesmo tipo de contato, a primeira adicionará o novo contato e todas as chamadas sucessivas para o mesmo Conta da AWS tipo de contato atualizarão o contato existente.

Example

O exemplo a seguir exclui o contato alternativo de segurança da conta do chamador.

```
$ aws account delete-alternate-contact \  
    --alternate-contact-type=SECURITY
```

Se for bem-sucedido, esse comando não produzirá uma saída.

Note

Se você tentar excluir o mesmo contato mais de uma vez, a primeira vez será bem-sucedida silenciosamente. Todas as tentativas posteriores geram uma exceção `ResourceNotFound`.

Atualize os contatos alternativos para qualquer Conta da AWS na sua organização

Para adicionar ou editar os detalhes de contato alternativos de qualquer Conta da AWS pessoa em sua organização, execute as etapas do procedimento a seguir.

Requisitos

Para atualizar contatos alternativos com o AWS Organizations console, você precisa fazer algumas configurações preliminares:

- A organização precisa habilitar todos os atributos para gerenciar as configurações das contas de membros. Isso permite o controle administrativo das contas-membro. Isso é definido por padrão quando você cria sua organização. Se sua organização estiver configurada somente para faturamento consolidado e você quiser habilitar todos os atributos, consulte [Enabling all features for an organization](#).

- Você precisa habilitar o acesso confiável ao serviço de gerenciamento de AWS contas. Para configurar isso, consulte [Habilite o acesso confiável para AWS Gerenciamento de contas](#).

Note

As políticas AWS Organizations `AWSOrganizationsReadOnlyAccess` gerenciadas `AWSOrganizationsFullAccess` são atualizadas para fornecer permissão para acessar as APIs de gerenciamento de AWS contas para que você possa acessar os dados da conta a partir do AWS Organizations console. Para ver as políticas gerenciadas atualizadas, consulte [Atualizações nas políticas AWS gerenciadas das organizações](#).

Console de gerenciamento da AWS

Para adicionar ou editar os contatos alternativos para qualquer Conta da AWS na sua organização

1. Faça login no [console do AWS Organizations](#) com as credenciais da conta de gerenciamento da organização.
2. Em Contas da AWS, selecione a conta que você deseja atualizar.
3. Escolha Informações de contato e, em Contatos alternativos, localize o tipo de contato: Contato de cobrança, Contato de segurança ou Contato de operações.
4. Para adicionar um novo contato, selecione Adicionar ou, para atualizar um contato existente, selecione Editar.
5. Altere os valores em qualquer um dos campos disponíveis.

Important

Para empresas Contas da AWS, é uma prática recomendada inserir um número de telefone e endereço de e-mail da empresa em vez de um pertencente a um indivíduo.

6. Depois de fazer todas as alterações, escolha Atualizar.

AWS CLI & SDKs

Você pode recuperar, atualizar ou excluir as informações de contato alternativas usando os seguintes AWS CLI comandos ou suas operações equivalentes no AWS SDK:

- [GetAlternateContact](#)
- [PutAlternateContact](#)
- [DeleteAlternateContact](#)

Observações

- Para executar realizar essas operações na conta de gerenciamento ou em uma conta de administrador delegado em uma organização em relação a contas-membro, você precisa [habilitar o acesso confiável ao serviço Conta](#).
- Você não pode acessar uma conta em uma organização diferente da que está usando para chamar a operação.

Permissões mínimas

Para cada operação, você deve ter a permissão que mapeia para essa operação:

- `GetAlternateContact` (para ver os detalhes dos contatos alternativos)
- `PutAlternateContact` (para definir ou atualizar um contato alternativo)
- `DeleteAlternateContact` (para excluir um contato alternativo)

Se você usar essas permissões individuais, poderá conceder a alguns usuários a capacidade de ler somente as informações de contato e conceder a outros a capacidade de ler e gravar.

Example

O exemplo a seguir recupera o contato alternativo de faturamento atual da conta do chamador de uma organização. As credenciais usadas devem pertencer à conta de gerenciamento da organização ou à conta de administrador delegado do serviço de Gerenciamento de Contas.

```
$ aws account get-alternate-contact \
  --alternate-contact-type=BILLING \
```

```
--account-id 123456789012

{
  "AlternateContact": {
    "AlternateContactType": "BILLING",
    "EmailAddress": "saanvi.sarkar@amazon.com",
    "Name": "Saarvi Sarkar",
    "PhoneNumber": "+1(206)555-0123",
    "Title": "CF0"
  }
}
```

Example

O exemplo a seguir define o contato alternativo das operações da conta-membro especificada em uma organização. As credenciais usadas devem pertencer à conta de gerenciamento da organização ou à conta de administrador delegado do serviço de Gerenciamento de Contas.

```
$ aws account put-alternate-contact \
  --account-id 123456789012 \
  --alternate-contact-type=OPERATIONS \
  --email-address=mateo_jackson@amazon.com \
  --name="Mateo Jackson" \
  --phone-number="+1(206)555-1234" \
  --title="Operations Manager"
```

Se for bem-sucedido, esse comando não produzirá uma saída.

Note

Se você realizar várias PutAlternateContact operações no mesmo Conta da AWS e no mesmo tipo de contato, a primeira adicionará o novo contato e todas as chamadas sucessivas para o mesmo Conta da AWS tipo de contato atualizarão o contato existente.

Example

O exemplo a seguir exclui o contato alternativo de segurança da conta-membro especificada em uma organização. As credenciais usadas devem pertencer à conta de gerenciamento da organização ou à conta de administrador delegado do serviço de Gerenciamento de Contas.

```
$ aws account delete-alternate-contact \
```

```
--account-id 123456789012 \  
--alternate-contact-type=SECURITY
```

Se for bem-sucedido, esse comando não produzirá uma saída.

Example

Note

Se você tentar excluir o mesmo contato mais de uma vez, a primeira vez será bem-sucedida silenciosamente. Todas as tentativas posteriores geram uma exceção `ResourceNotFound`.

conta: chave de AlternateContactTypes contexto

Você pode usar a chave de contexto `account:AlternateContactTypes` para especificar qual dos três tipos de contato é permitido (ou negado) pela política do IAM. O exemplo a seguir de política de permissão do IAM usa essa chave de condição para permitir que as entidades principais anexadas recuperem, mas não modifiquem, somente o contato alternativo BILLING de uma conta específica em uma organização.

Como `account:AlternateContactTypes` é um tipo de string multivalor, você deve usar os operadores de string de vários valores [ForAnyValue](#) ou [ForAllValues](#).

Atualize o contato principal do seu Conta da AWS

Essas instruções são sobre como atualizar o contato principal Conta da AWS se você se inscreveu para AWS usar a opção Inscrever-se em AWS (avançado) ou se ativou recursos avançados para sua conta. Para comparar as opções de inscrição, consulte [Compare as opções de inscrição](#).

É possível atualizar as informações do contato principal associadas à conta, inclusive o nome completo do contato, o nome da empresa, o endereço de correspondência, o número de telefone e endereço do site.

Você também pode verificar o número de telefone do contato principal. Para obter mais informações, consulte [Verifique o número de telefone do contato principal](#).

Você pode editar o contato principal da conta de forma diferente, dependendo se as contas são autônomas ou fazem parte de uma organização:

- **Independente Contas da AWS** — Se Contas da AWS não estiver associado a uma organização, você pode atualizar seu próprio contato de conta principal usando o AWS Management Console ou via AWS CLI e SDKs. Para saber como fazer isso, consulte [Atualizar contato Conta da AWS primário autônomo](#).
- **Contas da AWS dentro de uma organização** — Para contas de membros que fazem parte de uma AWS organização, um usuário na conta de gerenciamento ou na conta de administrador delegado pode atualizar centralmente qualquer conta membro na organização a partir do AWS Organizations console ou programaticamente por meio da CLI AWS e dos SDKs. Para saber como fazer isso, consulte [Atualizar o contato Conta da AWS principal em sua organização](#).

Tópicos

- [Requisitos de número de telefone e endereço de e-mail](#)
- [Atualizar o contato principal para um contato autônomo Conta da AWS ou conta de gerenciamento](#)
- [Atualize o contato principal para qualquer AWS conta de membro em sua organização](#)
- [Verifique o número de telefone do contato principal](#)

Requisitos de número de telefone e endereço de e-mail

Antes de prosseguir com a atualização das informações do contato principal da conta, recomendamos que você primeiro analise os requisitos a seguir quando inserir números de telefone e endereços de e-mail.

- Os números de telefone só devem conter números.
- Os números de telefone devem começar com + e o código do país e não devem ter zeros à esquerda ou espaços adicionais após o código do país. Por exemplo, +1 (US/Canada) ou +44 (Reino Unido).
- Os números de telefone não devem incluir espaços em branco entre o código de área, o código de troca e o código local. Por exemplo, +12025550179.
- Por motivos de segurança, os números de telefone devem ser capazes de receber SMS da AWS. Chamadas gratuitas não serão aceitas, pois a maioria não oferece suporte a SMS.
- Para empresas Contas da AWS, é uma prática recomendada inserir o número de telefone e o endereço de e-mail da empresa, em vez de um pertencente a uma pessoa física. Configurar o [usuário raiz](#) da conta com o endereço de e-mail ou número de telefone de um indivíduo pode dificultar a recuperação da sua conta se esse indivíduo deixar a empresa.

Atualizar o contato principal para um contato autônomo Conta da AWS ou conta de gerenciamento

Para editar seus detalhes de contato principais para uma conta autônoma Conta da AWS ou de gerenciamento, execute as etapas no procedimento a seguir. O Console de gerenciamento da AWS procedimento a seguir sempre funciona somente no contexto autônomo. Você pode usar o Console de gerenciamento da AWS para acessar ou alterar somente as informações do contato principal da conta que você usou para chamar a operação.

Console de gerenciamento da AWS

Para editar seu contato principal para um contato autônomo Conta da AWS ou conta de gerenciamento

Permissões mínimas

Para executar as etapas a seguir, é necessário ter as seguintes permissões do IAM:

- `account:GetContactInformation` (para ver os detalhes do contato principal)
- `account:PutContactInformation` (para atualizar os detalhes do contato principal)

1. Faça login no [Console de gerenciamento da AWS](#) como um usuário ou perfil do IAM que tenha as permissões mínimas.
2. Escolha o nome da conta no canto superior direito da janela e depois escolha Conta.
3. Role para baixo até a seção Informações de contato e, ao lado dela, escolha Editar.
4. Altere os valores em qualquer um dos campos disponíveis.
5. Depois de fazer todas as alterações, escolha Atualizar.

AWS CLI & SDKs

Você pode recuperar, atualizar ou excluir as informações de contato principais usando os seguintes AWS CLI comandos ou suas operações equivalentes no AWS SDK:

- [GetContactInformation](#)
- [PutContactInformation](#)

Observações

- Para executar realizar essas operações na conta de gerenciamento ou em uma conta de administrador delegado em uma organização em relação a contas-membro, você precisa [habilitar o acesso confiável ao serviço Conta](#).

Permissões mínimas

Para cada operação, você deve ter a permissão que mapeia para essa operação:

- `account:GetContactInformation`
- `account:PutContactInformation`

Se você usar essas permissões individuais, poderá conceder a alguns usuários a capacidade de ler somente as informações de contato e conceder a outros a capacidade de ler e gravar.

Example

O exemplo a seguir recupera as informações do contato principal atual da conta do chamador.

```
$ aws account get-contact-information
{
  "ContactInformation": {
    "AddressLine1": "123 Any Street",
    "City": "Seattle",
    "CompanyName": "Example Corp, Inc.",
    "CountryCode": "US",
    "DistrictOrCounty": "King",
    "FullName": "Saanvi Sarkar",
    "PhoneNumber": "+15555550100",
    "PostalCode": "98101",
    "StateOrRegion": "WA",
    "WebsiteUrl": "https://www.examplecorp.com"
  }
}
```

Example

O exemplo a seguir define as informações do novo contato principal da conta do chamador.

```
$ aws account put-contact-information --contact-information \
'{"AddressLine1": "123 Any Street", "City": "Seattle", "CompanyName": "Example Corp,
Inc.", "CountryCode": "US", "DistrictOrCounty": "King",
"FullName": "Saanvi Sarkar", "PhoneNumber": "+15555550100", "PostalCode": "98101",
"StateOrRegion": "WA", "WebsiteUrl": "https://www.examplecorp.com"}'
```

Se for bem-sucedido, esse comando não produzirá uma saída.

Atualize o contato principal para qualquer AWS conta de membro em sua organização

Para editar seus detalhes de contato principais em qualquer conta de AWS membro em sua organização, execute as etapas no procedimento a seguir.

Requisitos adicionais

Para atualizar o contato principal com o AWS Organizations console, você precisa fazer algumas configurações preliminares:

- A organização precisa habilitar todos os atributos para gerenciar as configurações das contas de membros. Isso permite o controle administrativo das contas-membro. Isso é definido por padrão quando você cria sua organização. Se sua organização estiver configurada somente para faturamento consolidado e você quiser habilitar todos os atributos, consulte [Enabling all features for an organization](#).
- Você precisa habilitar o acesso confiável para o serviço de gerenciamento de AWS contas. Para configurar isso, consulte [Habilite o acesso confiável para AWS Gerenciamento de contas](#).

Console de gerenciamento da AWS

Para editar seu contato principal para qualquer Conta da AWS na sua organização

1. Faça login no [console do AWS Organizations](#) com as credenciais da conta de gerenciamento da organização.
2. Em Contas da AWS, selecione a conta que você deseja atualizar.
3. Escolha Informações de contato e localize Contato principal.
4. Selecione Editar.

5. Altere os valores em qualquer um dos campos disponíveis.
6. Depois de fazer todas as alterações, escolha Salvar.

Se você alterar o número de telefone, enviaremos um código de verificação para o novo número quando você escolher Salvar. Você pode verificar o número imediatamente ou mais tarde. Para obter mais informações, consulte [Verifique o número de telefone de uma conta membro em sua organização](#).

AWS CLI & SDKs

Você pode recuperar, atualizar ou excluir as informações de contato principais usando os seguintes AWS CLI comandos ou suas operações equivalentes no AWS SDK:

- [GetContactInformation](#)
- [PutContactInformation](#)

Observações

- Para executar realizar essas operações na conta de gerenciamento ou em uma conta de administrador delegado em uma organização em relação a contas-membro, você precisa [habilitar o acesso confiável ao serviço Conta](#).
- Você não pode acessar uma conta em uma organização diferente daquela que você está usando para chamar a operação.

Permissões mínimas

Para cada operação, você deve ter a permissão que mapeia para essa operação:

- `account:GetContactInformation`
- `account:PutContactInformation`

Se você usar essas permissões individuais, poderá conceder a alguns usuários a capacidade de ler somente as informações de contato e conceder a outros a capacidade de ler e gravar.

Example

O exemplo a seguir recupera as informações do contato principal atual da conta-membro especificada em uma organização. As credenciais usadas devem pertencer à conta de gerenciamento da organização ou à conta de administrador delegado do serviço de Gerenciamento de Contas.

```
$ aws account get-contact-information --account-id 123456789012
{
  "ContactInformation": {
    "AddressLine1": "123 Any Street",
    "City": "Seattle",
    "CompanyName": "Example Corp, Inc.",
    "CountryCode": "US",
    "DistrictOrCounty": "King",
    "FullName": "Saanvi Sarkar",
    "PhoneNumber": "+15555550100",
    "PostalCode": "98101",
    "StateOrRegion": "WA",
    "WebsiteUrl": "https://www.examplecorp.com"
  }
}
```

Example

O exemplo a seguir define as informações do contato principal da conta-membro especificada em uma organização. As credenciais usadas devem pertencer à conta de gerenciamento da organização ou à conta de administrador delegado do serviço de Gerenciamento de Contas.

```
$ aws account put-contact-information --account-id 123456789012 \
--contact-information '{"AddressLine1": "123 Any Street", "City": "Seattle",
"CompanyName": "Example Corp, Inc.", "CountryCode": "US", "DistrictOrCounty":
"King",
"FullName": "Saanvi Sarkar", "PhoneNumber": "+15555550100", "PostalCode": "98101",
"StateOrRegion": "WA", "WebsiteUrl": "https://www.examplecorp.com"}'
```

Se for bem-sucedido, esse comando não produzirá uma saída.

Verifique o número de telefone do contato principal

Você pode verificar o número de telefone nas informações de contato primárias de um Conta da AWS. A verificação confirma que o número de telefone registrado pode receber nossas mensagens de texto SMS.

Quando você inicia a verificação, enviamos um código de verificação de 6 dígitos por mensagem de texto SMS para o número de telefone atualmente registrado na conta. Você não insere um número de telefone para iniciar a verificação. Para finalizar, você insere o código antes que ele expire.

Lembre-se do seguinte ao verificar um número de telefone:

- O código expira 5 minutos após o envio.
- Se você solicitar um novo código, os códigos que enviamos anteriormente não funcionarão mais.
- Se o código estiver incorreto ou tiver expirado, solicite um novo código e tente novamente.
- Se o número de telefone mudar depois de enviarmos um código, você não poderá usar esse código. Solicite um novo código para o número atual.
- O status da verificação sempre descreve o número de telefone atualmente registrado. Se você alterar o número de telefone, o status descreverá o novo número.
- Para uma conta membro em uma organização, o código vai para o número de telefone de contato principal da conta do membro, não para o seu. Antes de começar, verifique se você pode obter o código de quem tem esse telefone.

Para verificar o status da verificação, use a [GetContactInformation](#) operação. O `VerificationStatus` campo na resposta tem um dos seguintes valores:

- `VERIFIED`— O número de telefone registrado é verificado.
- `UNVERIFIED`— O número de telefone registrado não foi verificado.
- `NOT_SUPPORTED`— A verificação do número de telefone não está disponível para esta conta.

Verifique o número de telefone de um funcionário autônomo ou administrativo Conta da AWS

Para verificar o número de telefone da conta cujas credenciais você usa, use os AWS CLI comandos a seguir ou as operações equivalentes do AWS SDK:

- [SendPhoneNumberVerification](#)

- [VerifyPhoneNumber](#)

Permissões mínimas

Para cada operação, você deve ter a permissão que mapeia para essa operação:

- `account:SendPhoneNumberVerification`
- `account:VerifyPhoneNumber`

Para verificar o status da verificação, você também precisa `account:GetContactInformation`.

Example

O AWS CLI exemplo a seguir envia um código de verificação para o número de telefone do contato principal da conta do chamador:

```
$ aws account send-phone-number-verification
{
  "Status": "PENDING"
}
```

Example

O AWS CLI exemplo a seguir envia o código para concluir a verificação:

```
$ aws account verify-phone-number --otp 123456
{
  "Status": "VERIFIED"
}
```

Example

O AWS CLI exemplo a seguir recupera o status de verificação do número de telefone de contato principal do chamador:

```
$ aws account get-contact-information --query VerificationStatus
```


"VERIFIED"

Verifique o número de telefone de uma conta membro em sua organização

Você pode verificar o número de telefone de uma conta de membro usando o AWS Organizations console AWS CLI, o ou um AWS SDK. Antes de começar, conclua as etapas em [Requisitos adicionais](#).

Console de gerenciamento da AWS

Para verificar o número de telefone de contato principal de uma conta de membro

 Permissões mínimas

Para executar as etapas a seguir, é necessário ter as seguintes permissões do IAM:

- `account:GetContactInformation`(para ver o número de telefone e se ele foi verificado)
- `account:SendPhoneNumberVerification`(para enviar um código de verificação)
- `account:VerifyPhoneNumber`(para enviar o código)

A política `AWSOrganizationsFullAccess` gerenciada não inclui `account:SendPhoneNumberVerification` ou `account:VerifyPhoneNumber`. Se você confiar nessa política, conceda essas permissões separadamente.

1. Faça login no [console do AWS Organizations](#) com as credenciais da conta de gerenciamento da organização.
2. Contas da AWSEm, selecione a conta do membro.
3. Escolha Informações de contato e localize Contato principal.
4. Se o número de telefone não for verificado, ele aparecerá com um aviso. Escolha o número de telefone e, em seguida, escolha Verificar número de telefone. Enviamos um código de 6 dígitos para o número de telefone da conta do membro.
5. Insira o código em Código de verificação e escolha Verificar.

Se o código não chegar, escolha Reenviar código quando essa opção estiver disponível.

AWS CLI & SDKs

Para verificar o número de telefone da conta do membro, use os AWS CLI comandos a seguir ou as operações equivalentes do AWS SDK e especifique o ID da conta do membro:

- [SendPhoneNumberVerification](#)
- [VerifyPhoneNumber](#)

Observações

- As credenciais que você usa devem ser da conta de gerenciamento da organização ou da conta de administrador delegado para gerenciamento de AWS contas.
- Você não pode acessar uma conta em uma organização diferente daquela que você está usando para chamar a operação.

Permissões mínimas

Para cada operação, você deve ter a permissão que mapeia para essa operação:

- `account:SendPhoneNumberVerification`
- `account:VerifyPhoneNumber`

Para verificar o status da verificação, você também precisa `account:GetContactInformation`.

Example

O AWS CLI exemplo a seguir envia um código de verificação para o número de telefone do contato principal da conta de membro especificada:

```
$ aws account send-phone-number-verification --account-id 123456789012
{
  "Status": "PENDING"
}
```

Example

O AWS CLI exemplo a seguir envia o código que enviamos para o número de telefone da conta do membro:

```
$ aws account verify-phone-number --account-id 123456789012 --otp 123456
{
  "Status": "VERIFIED"
}
```

Visualizar Conta da AWS identificadores

Essas informações são sobre a visualização de Conta da AWS identificadores se você se inscreveu para AWS usar o Sign up for AWS (avançado) ou se tiver ativado recursos avançados para sua conta. Para comparar as opções de inscrição, consulte [Compare as opções de inscrição](#).

AWS atribui os seguintes identificadores exclusivos a cada um: Conta da AWS

[Conta da AWS ID](#)

Um número de 12 dígitos, como 012345678901, que identifica de forma exclusiva uma Conta da AWS. Muitos AWS recursos incluem o ID da conta em seus nomes de recursos [da Amazon \(ARNs\)](#). A parte do ID da conta distingue os recursos de uma conta dos recursos de outra conta. Se você for um usuário AWS Identity and Access Management (IAM), poderá fazer login no Console de gerenciamento da AWS usando o ID da conta ou o alias da conta. Embora os IDs de conta, assim como quaisquer informações de identificação, devam ser usados e compartilhados com cuidado, eles não são considerados informações secretas, sigilosas ou confidenciais.

[ID de usuário canônico](#)

Um identificador alfanumérico, como 79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be, que é uma forma ofuscada da ID. Conta da AWS Você pode usar esse ID para identificar um Conta da AWS ao conceder acesso entre contas a buckets e objetos usando o Amazon Simple Storage Service (Amazon S3). Você pode recuperar o ID de usuário canônico da Conta da AWS como o [usuário-raiz](#) ou um usuário do IAM.

Você deve estar autenticado com AWS para ver esses identificadores.

 Warning

Não forneça suas AWS credenciais (incluindo senhas e chaves de acesso) a terceiros que precisem de seus Conta da AWS identificadores para compartilhar AWS recursos com você. Fazer isso lhes daria o mesmo acesso ao Conta da AWS que você tem.

Encontre o seu Conta da AWS ID

Você pode encontrar o Conta da AWS ID usando o Console de gerenciamento da AWS ou o AWS Command Line Interface (AWS CLI). No console, a localização do ID da conta depende se você está conectado como usuário raiz ou usuário do IAM. O ID da conta é o mesmo se você estiver conectado como usuário raiz ou usuário do IAM.

Como encontrar o ID da conta como usuário-raiz

Console de gerenciamento da AWS

Para encontrar o seu Conta da AWS ID quando conectado como usuário root

 Permissões mínimas

Para executar as etapas a seguir, é necessário ter as seguintes permissões do IAM:

- Quando você faz login como o usuário-raiz, não precisa de quaisquer permissões do IAM.

1. No canto superior direito da barra de navegação, escolha o nome ou o número da conta e, em seguida, Credenciais de segurança.

 Tip

Se você não vir a opção credenciais de segurança, significa que poderá ter feito login como usuário federado com um perfil do IAM, em vez de como usuário do IAM. Nesse caso, procure a conta de entrada e o número do ID da conta ao lado dela.

2. Na seção Detalhes da conta, o número da conta aparece ao lado do ID da Conta da AWS .

AWS CLI & SDKs

Para encontrar seu Conta da AWS ID usando o AWS CLI

Permissões mínimas

Para executar as etapas a seguir, é necessário ter as seguintes permissões do IAM:

- Quando você executa o comando como o usuário-raiz, não precisa de quaisquer permissões do IAM.

Use o comando [get-caller-identity](#) como a seguir.

```
$ aws sts get-caller-identity \  
  --query Account \  
  --output text  
123456789012
```

Encontrar o ID da conta como usuário do IAM

Console de gerenciamento da AWS

Para encontrar o seu Conta da AWS ID quando conectado como usuário do IAM

Permissões mínimas

Para executar as etapas a seguir, é necessário ter as seguintes permissões do IAM:

- `account:GetAccountInformation`

1. No canto superior direito da barra de navegação, escolha seu nome de usuário e selecione Credenciais de segurança.

Tip

Se você não vir a opção credenciais de segurança, significa que poderá ter feito login como usuário federado com um perfil do IAM, em vez de como usuário do IAM. Nesse caso, procure a conta de entrada e o número do ID da conta ao lado dela.

2. Na parte superior da página, em Detalhes da conta, o número da conta aparece ao lado do ID da Conta da AWS .

AWS CLI & SDKs

Para encontrar seu Conta da AWS ID usando o AWS CLI

Permissões mínimas

Para executar as etapas a seguir, é necessário ter as seguintes permissões do IAM:

- Quando executa o comando como usuário ou perfil do IAM, você deve ter:
 - `sts:GetCallerIdentity`

Use o comando [get-caller-identity](#) como a seguir.

```
$ aws sts get-caller-identity \  
  --query Account \  
  --output text  
123456789012
```

Encontre o ID de usuário canônico para seu Conta da AWS

Você pode encontrar o ID de usuário canônico para você Conta da AWS usando o Console de gerenciamento da AWS ou o. AWS CLI O ID de usuário canônico de um Conta da AWS é específico para essa conta. Você pode recuperar o ID de usuário canônico para você Conta da AWS como usuário raiz, usuário federado ou usuário do IAM.

Encontrar o ID de usuário canônico como o usuário-raiz ou um usuário do IAM

Console de gerenciamento da AWS

Para encontrar o ID de usuário canônico da conta quando você tiver feito login no console como usuário-raiz ou um usuário do IAM

Permissões mínimas

Para executar as etapas a seguir, é necessário ter as seguintes permissões do IAM:

- Quando você executa o comando como o usuário-raiz, não precisa de quaisquer permissões do IAM.
- Quando fizer login como usuário do IAM, você deverá ter:
 - `account:GetAccountInformation`

1. Faça login no Console de gerenciamento da AWS como usuário root ou usuário do IAM.
2. No canto superior direito da barra de navegação, escolha o nome ou o número da conta e, em seguida, Credenciais de segurança.

Tip

Se você não vir a opção credenciais de segurança, significa que poderá ter feito login como usuário federado com um perfil do IAM, em vez de como usuário do IAM. Nesse caso, procure a conta de entrada e o número do ID da conta ao lado dela.

3. Na seção Detalhes da conta, o ID de usuário canônico aparece ao lado de ID de usuário canônico. Você pode usar o ID de usuário canônico para configurar listas de controle de acesso (ACLs) do Amazon S3.

AWS CLI & SDKs

Para encontrar o ID de usuário canônico usando o AWS CLI

O mesmo AWS CLI comando da API funciona para os Usuário raiz da conta da AWS usuários do IAM ou as funções do IAM.

Use o comando [list-buckets](#) como a seguir.

```
$ aws s3api list-buckets \
  --max-items 10 \
  --page-size 10 \
  --query Owner.ID \
  --output text
249fa2f1dc32c330EXAMPLE91b2778fcc65f980f9172f9cb9a5f50ccbEXAMPLE
```

Encontrar o ID canônico como um usuário federado com um perfil do IAM

Console de gerenciamento da AWS

Para encontrar o ID de usuário canônico da conta quando você tiver feito login no console como usuário federado com um perfil do IAM

Permissões mínimas

- Você deve ter permissão para listar e visualizar um bucket do Amazon S3.

1. Faça login no Console de gerenciamento da AWS como um usuário federado com uma função do IAM.
2. No console do Amazon S3, escolha um nome de bucket para visualizar os detalhes do bucket.
3. Escolha a aba Permissões.
4. Na seção Lista de controle de acesso, em Proprietário do bucket, é exibido o ID de usuário canônico da Conta da AWS .

AWS CLI & SDKs

Para encontrar o ID de usuário canônico usando o AWS CLI

O mesmo AWS CLI comando da API funciona para os Usuário raiz da conta da AWS usuários do IAM ou as funções do IAM.

Use o comando [list-buckets](#) como a seguir.

```
$ aws s3api list-buckets \
  --max-items 10 \
```



```
--page-size 10 \  
--query Owner.ID \  
--output text  
249fa2f1dc32c330EXAMPLE91b2778fcc65f980f9172f9cb9a5f50ccbEXAMPLE
```

Solucione o problema do seu Conta da AWS

Essas informações são sobre como solucionar problemas Conta da AWS se você se inscreveu para AWS usar o Sign up for AWS (avançado) ou se ativou recursos avançados para sua conta. Para comparar as opções de inscrição, consulte [Compare as opções de inscrição](#).

Use as informações dos tópicos a seguir para ajudar no diagnóstico e na correção de problemas com a Conta da AWS. Para obter ajuda com o usuário-raiz, consulte [Solucionar problemas com o usuário-raiz](#) no Guia do usuário do IAM. Para obter ajuda com o processo de login, consulte [Solução de problemas de Conta da AWS login no Guia do usuário](#). AWS Sign-In

Tópicos de solução de problemas

- [Solução de problemas com Conta da AWS criação](#)
- [Solução de problemas com Conta da AWS encerramento](#)
- [Solucionando outros problemas com Contas da AWS](#)

Solução de problemas com Conta da AWS criação

Essas informações são sobre como solucionar problemas de Conta da AWS criação se você se inscreveu para AWS usar o Sign up for AWS (avançado) ou se tiver ativado recursos avançados para sua conta. Para comparar as opções de inscrição, consulte [Compare as opções de inscrição](#).

Use os links de referência na tabela a seguir para ajudá-lo a diagnosticar e corrigir problemas na criação de um novo Conta da AWS.

Problema	Link de referência	Fonte
Não sei como me cadastrar ou criar uma conta	Inscreva-se para AWS (avançado)	Este guia
O que devo fazer se eu não receber uma ligação AWS	https://repost.aws/knowledge-center/phone-verify-no-call	AWS re:Post

Problema	Link de referência	Fonte
para verificar minha nova conta ou se o PIN que inseri não funcionar?		
Como resolvo o erro de “número máximo de tentativas fracassadas” quando tento verificar minhas tentativas Conta da AWS por telefone?	https://repost.aws/knowledge-center/maximum-failed-attempts	AWS re:Post
Já se passaram mais de 24 horas e minha conta não está ativada	https://repost.aws/knowledge-center/create-and-activate-aws-account	AWS re:Post
Não consigo fazer login na nova conta depois que ela foi criada	https://docs.aws.amazon.com/signin/latest/userguide/troubleshooting-sign-in-issues.html	AWS Sign-In Guia do usuário

Para obter ajuda adicional, recomendamos que você pesquise o [AWS re:Post](#) para conhecer o conteúdo relacionado ao seu problema específico. Se você ainda precisar de assistência, entre em contato com o [AWS Support](#).

Solução de problemas com Conta da AWS encerramento

Essas informações são sobre como solucionar problemas de Conta da AWS encerramento se você se inscreveu para AWS usar o Sign up for AWS (avançado) ou se tiver ativado recursos avançados para sua conta. Para comparar as opções de inscrição, consulte [Compare as opções de inscrição](#).

Use as informações abaixo para obter ajuda no diagnóstico e na correção de problemas comuns encontrados durante o processo de encerramento da conta. Para obter informações gerais sobre o processo de encerramento da conta, consulte [Fechar um Conta da AWS](#).

Tópicos

- [Não sei como excluir ou cancelar a conta](#)
- [Não vejo o botão Encerrar conta na página Contas](#)
- [Encerrei minha conta, mas ainda não recebi uma confirmação por e-mail](#)

- [Eu recebo um erro ConstraintViolationException "" ao tentar fechar minha conta](#)
- [Recebo o erro "CLOSE_ACCOUNT_QUOTA_EXCEEDED" ao tentar encerrar uma conta-membro](#)
- [Preciso excluir meu AWS organização antes de fechar a conta de gerenciamento?](#)

Não sei como excluir ou cancelar a conta

Para encerrar a conta, siga as instruções em [Fechar um Conta da AWS](#).

Não vejo o botão Encerrar conta na página Contas

Se sua conexão não for como usuário-raiz, o botão Encerrar conta não será exibido na página Contas. Você deve fazer [login no Console de gerenciamento da AWS como usuário root](#) para fechar sua conta. Se você não conseguir fazer login, consulte [Solucionar problemas com o usuário-raiz](#).

Encerrei minha conta, mas ainda não recebi uma confirmação por e-mail

Essa confirmação por e-mail só é enviada ao endereço de e-mail do usuário-raiz para sua Conta da AWS. Se você não receber esse e-mail em algumas horas, faça [login no Console de gerenciamento da AWS como usuário root](#) para verificar se sua conta está fechada. Se a conta tiver sido encerrada com êxito, será exibida uma mensagem indicando que a conta foi encerrada. Se a conta que você fechou for uma conta de membro, você poderá verificar o encerramento bem-sucedido verificando se a conta fechada está rotulada como CLOSED no AWS Organizations console. Para obter mais informações, consulte [Fechar uma conta-membro na sua organização](#) no Guia do usuário do AWS Organizations .

Se você estiver tentando encerrar uma conta de gerenciamento e não receber uma confirmação por e-mail sobre o encerramento da conta, provavelmente a organização tem contas-membro ativas. Você só poderá encerrar a conta de gerenciamento se a organização não tiver contas-membro ativas. Para verificar se não há contas de membros ativas restantes em sua organização, acesse o AWS Organizations console e verifique se todas as contas de membros estão aparecendo ao Closed lado dos nomes de suas contas. Depois disso, você pode encerrar a conta de gerenciamento.

Eu recebo um erro ConstraintViolationException "" ao tentar fechar minha conta

Você está tentando fechar uma conta de gerenciamento usando o AWS Organizations console, o que não é possível. Para fechar uma conta de gerenciamento, você precisa fazer [login no Console](#)

[de gerenciamento da AWS como usuário](#) raiz da conta de gerenciamento e fechá-la na página Contas. Para obter mais informações, consulte [Closing a management account in your organization](#) no AWS Organizations User Guide.

Recebo o erro “CLOSE_ACCOUNT_QUOTA_EXCEEDED” ao tentar encerrar uma conta-membro

Você só pode fechar 20% das contas dos membros dentro de um período contínuo de 30 dias. Essa cota não está associada a um mês do calendário. A contagem começa assim que você encerra uma conta. Dentro de 30 dias após o encerramento inicial da conta, você não pode exceder o limite de 20% de encerramento da conta. O encerramento mínimo da conta é 250 e o encerramento máximo da conta é 1000, mesmo que 20% das contas excedam 1000. Para obter mais informações sobre cotas do Organizations, consulte [Quotas for AWS Organizations](#) no AWS Organizations User Guide.

Preciso excluir meu AWS organização antes de fechar a conta de gerenciamento?

Não, você não precisa excluir sua AWS organização antes de fechar a conta de gerenciamento. Entretanto, você só poderá encerrar a conta de gerenciamento se a organização não tiver contas-membro ativas. Para verificar se não há contas de membros ativas restantes em sua organização, acesse o AWS Organizations console e verifique se todas as contas de membros estão aparecendo ao Closed lado dos nomes de suas contas. Depois disso, você pode encerrar a conta de gerenciamento.

Solucionando outros problemas com Contas da AWS

Essas informações são para solucionar outros problemas Conta da AWS se você se inscreveu para AWS usar o Cadastre-se para AWS (avançado) ou se ativou recursos avançados para sua conta. Para comparar as opções de inscrição, consulte [Compare as opções de inscrição](#).

Use as informações aqui contidas para obter ajuda para solucionar problemas relacionados à Conta da AWS.

Problemas

- [Preciso trocar o cartão de crédito do meu Conta da AWS](#)
- [Preciso denunciar uma fraude Conta da AWS atividade](#)
- [Eu preciso fechar meu Conta da AWS](#)
- [Eu recebo um AccessDeniedException quando atualizo o endereço de e-mail de um usuário root](#)

Preciso trocar o cartão de crédito do meu Conta da AWS

Para alterar o cartão de crédito do seu Conta da AWS, você deve conseguir fazer login. AWS tem proteções em vigor que exigem que você prove que é o proprietário da conta. Para obter instruções, consulte [Gerenciar métodos de pagamento de cartão de crédito](#) no Guia do usuário do AWS Billing .

Preciso denunciar uma fraude Conta da AWS atividade

Se você suspeitar de atividade fraudulenta usando o seu Conta da AWS e quiser fazer uma denúncia, consulte [Como faço para denunciar o abuso de AWS recursos](#).

Se você está tendo problemas com uma compra feita em Amazon.com, consulte o [Serviço de Atendimento ao Cliente da Amazon](#).

Eu preciso fechar meu Conta da AWS

Para obter ajuda na solução de problemas com o fechamento do seu Conta da AWS, consulte [Fechar um Conta da AWS](#).

Eu recebo um **AccessDeniedException** quando atualizo o endereço de e-mail de um usuário root

Se a conta do membro for uma conta do projeto, você não poderá atualizar o endereço de e-mail do usuário raiz. Uma ID do AWS Builder é proprietária de cada conta do projeto em vez do endereço de e-mail do usuário raiz. Para obter mais informações, consulte [Contas do projeto depois de ativar os recursos avançados](#).

Gerenciar contas na Índia

Essas informações são sobre o gerenciamento de contas na Índia, se você se inscreveu AWS para usar a opção Inscrever-se AWS em (avançado) ou se ativou recursos avançados para sua conta. Para comparar as opções de inscrição, consulte [Compare as opções de inscrição](#).

Se você se inscrever em um novo Conta da AWS e escolher a Índia como seu endereço de contato e cobrança, seu contrato de usuário será com a Amazon Web Services India Private Limited (AWS Índia), um AWS vendedor local na Índia. AWS A Índia gerencia seu faturamento e o total da fatura é listado em rúpias indianas (INR) em vez de dólares americanos (USD). Para obter informações sobre como gerenciar um Conta da AWS, consulte [Configure seu Conta da AWS](#).

Se sua conta estiver AWS na Índia, siga os procedimentos neste tópico para gerenciar sua conta. Este tópico explica como se inscrever em uma conta AWS na Índia, editar informações sobre AWS sua conta na Índia, gerenciar a verificação de clientes e adicionar ou editar seu Número de Conta Permanente (PAN).

Como parte da verificação do cartão de crédito durante a inscrição, a AWS Índia cobra 2 INR do seu cartão de crédito. AWS A Índia reembolsa os 2 INR após a verificação ser feita. Você pode ser redirecionado para seu banco como parte do processo de verificação.

Tópicos

- [Crie um Conta da AWS por AWS Índia](#)
- [Gerenciar suas informações de verificação do cliente](#)

Crie um Conta da AWS por AWS Índia

AWS A Índia é um vendedor local AWS de na Índia. Se seu endereço de contato e cobrança estiver na Índia e você quiser criar uma conta, use o procedimento a seguir para se inscrever em uma conta na AWS Índia.

Para se inscrever em um AWS Conta na Índia

1. Abra a [página inicial da Amazon Web Services](#).
2. Escolha Criar um Conta da AWS.

Note

Se você AWS fez login recentemente, essa opção pode não estar lá. Em vez disso, escolha Fazer login no console. Se a opção Criar uma nova Conta da AWS ainda não estiver exibida, escolha Fazer login em uma conta diferente e, em seguida, escolha Criar uma nova Conta da AWS.

3. Insira as informações da conta, verifique o endereço de e-mail e escolha uma senha forte para a conta.
4. Escolha Comercial ou Pessoal. Contas pessoais e comerciais têm os mesmos recursos e funções.
5. Insira suas informações de contato pessoais ou da empresa. Se seu endereço de contato ou cobrança estiver localizado na Índia, em conformidade com os regulamentos da Equipe Indiana

de Resposta a Emergências de Computadores (CERT-In), AWS é necessário coletar e validar suas informações de identidade antes de conceder acesso aos serviços. AWS

O nome que você escolher entre suas informações de contato ou de cobrança deve corresponder exatamente ao nome que aparece no documento que você planeja usar para a verificação do cliente. Por exemplo, se você planeja verificar uma conta comercial usando um Certificado de Incorporação social, deve fornecer o nome comercial que consta do documento. Para obter uma lista dos tipos de documentos aceitos, consulte [the section called “Documentos da Índia aceitos para verificação do cliente”](#).

6. Depois de ler o contrato de cliente, marque a caixa de seleção referente aos termos e condições e escolha Continuar.
7. Na página Billing information (Informações de faturamento), insira o método de pagamento que deseja usar. É necessário fornecer o CVV como parte do processo de verificação.
8. Em Você tem um PAN?, escolha Sim se você tiver um número de conta permanente (PAN) que gostaria que fosse exibido nas notas fiscais e, em seguida, insira o PAN. Se você não tiver um PAN ou se quiser adicioná-lo após o cadastro, escolha Não.
9. Escolha Verificar e continuar. AWS A Índia cobra 2 INR do seu cartão como parte do processo de verificação. AWS A Índia reembolsa os 2 INR após a verificação ser feita.
10. Na página Confirmar sua identidade, selecione o objetivo principal do registro da conta.
11. Escolha o tipo de propriedade que representa melhor o proprietário da conta. Se você escolher uma empresa, organização ou parceria como tipo de propriedade, insira o nome de um dos principais membros da administração. Essa pessoa pode ser um diretor, um chefe de operações ou uma pessoa responsável pelas operações da empresa.
12. Dependendo do tipo de propriedade selecionado, escolha um tipo de documento aceito na Índia para usar na verificação e insira as informações do documento.

 Note

Se você tem uma conta pessoal e planeja usar uma carteira de habilitação que não seja emitida pela União da Índia, é recomendável usar um tipo de documento pessoal diferente para verificação.

13. Escolha o nome que você deseja usar para verificação do cliente.

Os nomes das suas informações de faturamento e contato serão exibidos para seleção se estiverem associados a um endereço indiano. Certifique-se de que o nome que você

escolher corresponda ao nome que consta do tipo de documento que você planeja usar para a verificação do cliente. Se você precisar fazer alterações no nome associado ao endereço de faturamento ou contato, poderá fazer isso depois de concluir o cadastramento na conta.

14. Forneça seu consentimento para enviar as informações para verificação e escolha Continuar.

Você receberá uma notificação sobre o resultado da verificação do cliente por e-mail depois de concluir o cadastro na conta. Você também pode verificar o status na página de verificação do cliente nas configurações da sua conta ou no AWS Health Dashboard posteriormente. Você deve passar na verificação do cliente para acessar os serviços da AWS .

15. Escolha se deseja verificar o número do seu celular por Mensagem de texto (SMS) ou Chamada de voz.
16. Escolha seu país ou código de região e, em seguida, insira seu número de celular.
17. Complete a verificação de segurança.
18. Escolha Enviar SMS ou Ligar para mim agora. Depois de alguns momentos, você receberá um pin de quatro dígitos em um SMS ou em uma chamada automatizada no celular.
19. Na página Confirmar sua identidade, insira o pin que você recebeu e escolha Continuar.
20. Na página Selecione um plano de suporte, selecione o plano de suporte e, em seguida, escolha Concluir cadastramento. Depois que sua forma de pagamento e a verificação do cliente forem verificadas, sua conta será ativada e você receberá um e-mail confirmando a ativação de sua conta.

Note

Se você tiver concluído a verificação do cliente e tiver editado o nome, o endereço ou o tipo de documento anteriormente usado para verificar sua identidade, talvez seja necessário passar pela verificação do cliente novamente. Para obter mais informações, consulte [the section called “Editar suas informações de verificação do cliente”](#).

Gerenciar suas informações de verificação do cliente

Em conformidade com os regulamentos da Equipe Indiana de Resposta a Emergências de Computadores (CERT-In), AWS é necessário coletar e validar suas informações de identidade antes de conceder a você acesso novo ou contínuo aos AWS serviços. Sua identidade deve ser verificada usando o nome fornecido por você no endereço de faturamento ou de contato na Índia. Durante a verificação, AWS verificará se o número do documento é válido e se o nome fornecido corresponde

ao nome associado ao documento usado para verificação do cliente. O nome que você escolher para informações de contato ou faturamento deverá corresponder exatamente ao nome que consta do documento.

Para atualizar seu nome e endereço de faturamento, consulte a página [Preferências de pagamento](#). Para atualizar seu nome e endereço de contato, consulte [the section called “Atualize o contato principal do seu Conta da AWS”](#). Se você editar qualquer informação usada anteriormente para verificação do cliente, como nome ou India-based endereço das informações de contato ou cobrança, talvez seja necessário atualizar e reenviar as informações de verificação do cliente.

Verificar o status da sua verificação do cliente

Você pode verificar o status da sua verificação do cliente a qualquer momento na página Verificação do cliente. Se o status da sua verificação for Verificação necessária ou Falha na verificação, crie ou atualize suas informações de verificação do cliente e envie-as novamente para verificação.

Se sua conta de gerenciamento habilitou a herança de verificação do cliente, o status de verificação da sua conta refletirá o status dessa conta. Você não precisa realizar nenhuma ação quando a herança está ativa.

Criar suas informações de verificação do cliente

Para concluir a verificação do cliente, você precisará fornecer informações de um documento aceito na Índia. Para obter uma lista dos tipos de documentos aceitos, consulte [the section called “Documentos da Índia aceitos para verificação do cliente”](#).

1. Faça login no [Console de gerenciamento da AWS](#).
2. No canto superior direito da barra de navegação, escolha o nome (ou alias) da conta e escolha Conta.
3. Em Other settings (Outras configurações), escolha Customer verification (Verificação do cliente).

Se você ainda não tiver fornecido as informações de verificação do cliente, a página Criar verificação do cliente será exibida.

4. Escolha um nome que corresponda exatamente ao nome que consta do documento que você planeja usar para a verificação do cliente. Por exemplo, se você planeja verificar uma conta comercial usando um Certificado de Incorporação social, deve fornecer o nome comercial que consta do documento.
5. Forneça as informações remanescentes solicitadas na página. Dependendo do tipo de documento escolhido, talvez seja necessário carregar uma cópia da frente e do verso do

documento. Se você carregar um arquivo de imagem, verifique se todas as informações constantes do documento estão visíveis e legíveis.

6. Selecione Enviar.

Você será notificado sobre o resultado da verificação do cliente e sobre as próximas etapas por e-mail ou no AWS Health Dashboard.

Editar suas informações de verificação do cliente

Você pode editar suas informações de verificação do cliente, como o objetivo principal do registro da conta, o tipo de organização e o nome, o tipo de documento, o carregamento do documento ou as informações do documento que você deseja usar para verificação.

Se você editar o nome ou o tipo de documento a ser usado na verificação do cliente ou atualizar qualquer informação do documento, deverá verificar sua identidade novamente ao salvar as alterações.

Verificação: a herança está ativa

Se sua conta de gerenciamento tiver habilitado a herança de verificação do cliente, você não poderá editar ou enviar suas próprias informações de verificação do cliente. Suas informações de verificação aparecem no modo somente leitura.

1. Faça login no [Console de gerenciamento da AWS](#).
2. No canto superior direito da barra de navegação, escolha o nome (ou alias) da conta e escolha Conta.
3. Em Other settings (Outras configurações), escolha Customer verification (Verificação do cliente).
4. Escolha Editar e, em seguida, atualize as informações que você deseja alterar.

Ao atualizar as informações, observe as seguintes orientações:

- Se você escolher um nome diferente, o nome deverá corresponder exatamente ao nome que consta do documento que você planeja usar para a verificação do cliente. Por exemplo, se você planeja verificar uma conta comercial usando um Certificado de Incorporação social, deve fornecer o nome comercial que consta do documento.

- Se você escolher um tipo de documento diferente, precisará carregar uma cópia da frente e do verso (se aplicável) do documento. Todas as informações no carregamento do documento devem estar visíveis e legíveis.
- Se você tem uma conta pessoal e planeja usar uma carteira de habilitação que não seja emitida pela União da Índia, é recomendável usar um tipo de documento pessoal diferente para verificação.

Para obter uma lista dos tipos de documentos aceitos, consulte [the section called “Documentos da Índia aceitos para verificação do cliente”](#).

5. Selecione Enviar.

Se sua identidade precisar ser verificada novamente devido ao tipo de alteração que você salvou, você receberá uma notificação do resultado da verificação do cliente e das próximas etapas por e-mail. Você também pode ver os resultados retornando à página de verificação do cliente ou ao AWS Health Dashboard.

Gerencie a herança de verificação do cliente para AWS Organizações

Com o [AWS Organizations](#), você pode ativar a herança de verificação do cliente para sua organização. Quando você ativa a herança, as contas India-based dos membros da sua organização herdam o status de verificação da sua conta de gerenciamento. Eles não precisam concluir a verificação do cliente de forma independente.

Sua conta de gerenciamento deve concluir sua própria verificação de cliente antes de permitir a herança. Depois de habilitar a herança, você não precisa reenviar seus documentos de verificação.

Quando sua conta de gerenciamento permite a herança de verificação do cliente, seu status de verificação se estende às contas India-based dos membros em sua organização. Para essas contas de membros, podemos usar ou divulgar suas informações de verificação em resposta a solicitações policiais ou regulatórias.

Ativar ou desativar a herança de verificação do cliente

Use o procedimento a seguir para ativar ou desativar a herança de verificação do cliente para as contas dos India-based membros da sua organização.

1. Abra o Console de gerenciamento da AWS chapéu [Console de gerenciamento da AWS](#).
2. Na barra de navegação, escolha o nome da sua conta (ou alias) e, em seguida, escolha Conta.

3. Em **Other settings** (Outras configurações), escolha **Customer verification** (Verificação do cliente).
4. Em **Configurações de verificação do cliente**, ative a opção **Herança** para ativar a herança ou desative para desativá-la.
5. Revise a caixa de diálogo de confirmação e confirme sua escolha.

Quando você ativa a herança, todas as contas de Índia-based membros em sua organização herdam seu status de verificação. Quando você desativa a herança, restauramos o status de verificação anterior para contas de membros que concluíram anteriormente sua própria verificação. Uma conta de membro sem verificação prévia deve concluir a verificação do cliente de forma independente.

Verificação do cliente para AWS Contas de membros da Organizations

Se sua conta tiver um endereço de Índia-based contato ou de cobrança, você herdará o status de verificação da conta de gerenciamento. Isso se aplica quando sua conta de gerenciamento habilita a verificação da herança do cliente. Você pode ver uma mensagem na página de verificação do cliente que confirma isso.

Quando a herança está ativa, você não pode enviar ou editar suas próprias informações de verificação do cliente. Você não precisa realizar nenhuma ação.

Se sua conta de gerenciamento desabilitar a herança, você deverá ter seu próprio status de verificação de cliente. O mesmo se aplica se sua conta sair da organização ou se a conta de gerenciamento remover sua conta da organização. Se você enviou anteriormente suas próprias informações de verificação, restauramos seu status de verificação anterior. Você não precisa repetir o processo. Essa restauração se aplica somente se seu nome e endereço não tiverem sido alterados desde sua última verificação.

Documentos da Índia aceitos para verificação do cliente

Os seguintes tipos de documentos emitidos pelo governo indiano são aceitos para verificação do cliente.

Note

Os links a seguir estão sujeitos a alterações pelo governo.

- **Cartão de PAN:** disponível em formato digital e físico, o cartão de número de conta permanente (PAN) contém um identificador alfanumérico exclusivo emitido pelo Income Tax Department of

Índia para indivíduos, empresas e entidades. Um PAN consiste em dez caracteres, incluindo letras e números, no formato **AAAAA1111A**. Para usar esse documento para verificação, você também deve fornecer a data de nascimento (pessoa física) ou a data de incorporação (empresa) exibida no cartão de PAN e carregar a frente do cartão. Consulte o [site oficial do Income Tax Department](#) para verificar a validade do PAN.

- Identificação do eleitor Card/EPIC - A carteira de eleitor, também conhecida como Carteira de Identidade com Foto do Eleitor (EPIC), contém um número de identificação exclusivo emitido pela Comissão Eleitoral da Índia para eleitores elegíveis na Índia. O ID/EPIC número do eleitor consiste em dez caracteres, incluindo letras e números. Você pode acessar o site oficial da [Comissão Eleitoral da Índia](#) para verificar a validade da sua carteira de eleitor. Para usar esse documento para verificação, você deve carregar a frente e o verso do cartão.
- Carteira de habilitação: se sua carteira de habilitação não for emitida pela União da Índia, recomendamos o uso de um tipo de documento diferente para verificação. O número da carteira de habilitação consiste em 12 a 16 caracteres, incluindo letras, números e um espaço ou hífen. Para usar esse documento para verificação, você deve informar sua data de nascimento e carregar a frente e o verso do cartão. Acesse o [site Parivahan Sewa](#) do Ministry of Road Transport and Highways para verificar a validade da sua carteira de habilitação.
- Certificado de Incorporação: um certificado de incorporação é um documento emitido pelo Ministry of Corporate Affairs (MCA), que data o registro de uma empresa como pessoa jurídica. O certificado é usado para identificar e rastrear de forma exclusiva empresas registradas na Índia. Cada certificado contém um Número de Identificação Corporativa (CIN), que é um identificador alfanumérico exclusivo que consiste em 21 caracteres, incluindo letras e números. Para usar esse documento para verificação, você deve carregar o documento do certificado de incorporação. Você pode acessar o [portal do Ministry of Corporate Affairs](#) para verificar a validade do CIN.

Diferentes tipos de documentos da Índia são aceitos para contas pessoais e comerciais:

- Para contas pessoais - cartão PAN, carteira de eleitor e carteira de habilitação. card/EPIC
- Para contas comerciais: cartão de PAN e certificado de incorporação.

Gerencie seu AWS Conta na Índia

Com exceção das tarefas a seguir, os procedimentos para o gerenciamento da conta são os mesmos das contas criadas fora da Índia. Para obter informações gerais sobre como gerenciar a conta, consulte [the section called “Configurar a conta”](#).

Use o Console de gerenciamento da AWS para realizar as seguintes tarefas:

- [Adicionar ou editar um número de conta permanente](#)
- [Editar vários números de conta permanente](#)
- [the section called “Gerenciar suas informações de verificação do cliente”](#)
- [Editar vários números de imposto sobre bens e serviços \(GSTs\)](#)
- [Visualizar uma fatura fiscal](#)

Fechar um Conta da AWS

Estas instruções explicam como encerrar sua conta Conta da AWS se você se inscreveu para AWS usar a opção Inscrever-se em AWS (avançado) ou se ativou recursos avançados em sua conta. Para comparar as opções de inscrição, consulte [Compare as opções de inscrição](#).

Se você não precisar mais do seu Conta da AWS, poderá fechá-lo a qualquer momento seguindo as instruções nesta seção. Depois do encerramento da conta, você pode reabri-la até 90 dias a partir do dia do encerramento da conta. O período entre o dia em que você fechou a conta e o encerramento AWS permanente da conta é chamado de [período pós-fechamento](#).

O que você precisa saber antes de encerrar a conta

Antes de fechar o seu Conta da AWS, você deve considerar o seguinte:

- O encerramento da conta servirá como seu aviso de rescisão do Contrato de Cliente da AWS para esta conta.
- Você não precisa excluir recursos do seu Conta da AWS antes de fechá-lo. No entanto, recomendamos que você faça backup de todos os recursos ou dados que deseja manter. Para obter instruções sobre como fazer backup de um recurso específico, consulte a [documentação da AWS](#) apropriada desse serviço.
- Você pode reabrir a conta durante o período [pós-encerramento](#). As cobranças pelos serviços que permaneceram na conta serão reiniciadas se você reabri-la. Você também permanece responsável por quaisquer faturas não pagas e por [Instâncias Reservadas](#) e [Savings Plans](#) pendentes.
- Você permanece responsável por todas as taxas e cobranças pendentes pelos serviços consumidos antes do encerramento da conta. Você receberá uma AWS fatura no mês seguinte após o encerramento da conta. Por exemplo, se você tiver fechado a conta em 15 de janeiro,

receberá uma fatura no início de fevereiro pelo uso incorrido de 1.º de janeiro a 15 de janeiro. Você continuará recebendo faturas de [instâncias reservadas](#) e de [Savings Plans](#) depois de encerrar a conta até que eles expirem.

- Você não poderá mais acessar os AWS serviços que estavam disponíveis anteriormente em sua conta. No entanto, você pode fazer login e acessar uma conta fechada Conta da AWS durante o [período pós-encerramento](#) apenas para ver informações de cobrança anteriores, acessar as configurações da conta ou o contato. [AWS Support](#)
- Não é possível usar o mesmo endereço de e-mail registrado na Conta da AWS no momento do encerramento como e-mail principal de outra Conta da AWS. Se você quiser usar o mesmo endereço de e-mail para uma Conta da AWS diferente, recomendamos atualizá-lo antes do encerramento. Para obter mais informações, consulte [Atualize o endereço de e-mail do usuário-raiz](#).
- Você não pode usar o mesmo alias de conta que você registrou Conta da AWS no momento do encerramento para outra Conta da AWS. Para reutilizar o alias para outro Conta da AWS, exclua o alias da conta antes de fechar a conta. Para obter mais informações, consulte Como [usar um alias para seu Conta da AWS ID](#) no Guia do usuário do IAM.
- Se você tiver [habilitado autenticação multifator \(MFA\)](#) no usuário-raiz da Conta da AWS ou tiver configurado o [dispositivo com MFA em um usuário do IAM](#), a MFA não será removida automaticamente quando você encerrar a conta. Se você optar por deixar a MFA ativada durante o [período pós-encerramento](#) de 90 dias, mantenha o dispositivo com MFA ativo até que o período pós-encerramento expire, caso você precise acessar a conta durante esse período. Observe que os dispositivos token TOTP de hardware não podem ser associados a outro usuário após o encerramento permanente da conta. Se você quiser usar o token TOTP de hardware com outro usuário posteriormente, terá a opção de [desativar o dispositivo com MFA de hardware](#) antes de encerrar a conta. Os dispositivos com MFA para [usuários do IAM](#) devem ser excluídos pelo administrador da conta.

Considerações adicionais para contas-membro

- Quando uma conta-membro for encerrada, ela só será removida da organização do [período pós-encerramento](#). Durante o período pós-encerramento, uma conta de membro encerrada ainda será considerada na cota de contas na organização. Para evitar que a conta seja considerada na cota, consulte [Remove a member account from your organization](#) antes de encerrá-la.
- Você só pode fechar 20% ou 250 das contas dos membros até um máximo de 1.000 em um período contínuo de 30 dias, o que for maior. Essa cota não está associada a um mês do

calendário. A contagem começa assim que você encerra uma conta. Para obter mais informações sobre as cotas do Organizations, consulte [Quotas for AWS Organizations](#).

- Se você usa o AWS Control Tower, precisa desgerenciar a conta do membro antes de tentar fechá-la. Consulte [Unmanage a member account](#) (Remover o gerenciamento de uma conta-membro) no Guia do usuário do AWS Control Tower.

Considerações específicas do serviço

- AWS Marketplace as assinaturas não são canceladas automaticamente no encerramento da conta. Se você tiver assinaturas, primeiro [encerre todas as instâncias do software](#) nas assinaturas. Em seguida, acesse a página [Gerenciar assinaturas](#) do AWS Marketplace console e cancele suas assinaturas.
- Depois que uma conta for fechada, AWS enviaremos e-mails diários por até cinco dias antes de suspendermos o domínio. Depois que o domínio tiver sido suspenso e, dependendo do registrador do domínio, excluiríamos o domínio em 30 dias ou liberaremos o domínio para o registrador. Para obter mais informações, consulte [Meu Conta da AWS está fechado ou fechado permanentemente e meu domínio está registrado no Route 53](#).

Se o endereço de e-mail do usuário raiz dessa conta usar um domínio registrado pelo Route 53 nessa mesma conta, não feche essa conta até concluir uma das seguintes ações: transferir o domínio para outro Conta da AWS ou atualizar o endereço de e-mail do usuário raiz para usar um domínio que não esteja registrado nessa conta. Caso contrário, o fechamento da conta suspende o domínio, o que interrompe a entrega de e-mail para seu endereço de usuário raiz. Sem e-mail, você não pode recuperar a conta e, sem a conta, não é possível restabelecer o domínio. Depois de 30 dias, o Route 53 exclui permanentemente o domínio. Isso também se aplica às contas de membros cujos endereços de e-mail do usuário raiz usam domínios registrados nessa conta.

- AWS CloudTrail é um serviço de segurança fundamental. Isso significa que as trilhas criadas pelos usuários podem continuar existindo e entregando eventos mesmo após o fechamento de uma Conta da AWS, a menos que um usuário exclua explicitamente as trilhas Conta da AWS antes de fechá-las. Para obter mais informações sobre como solicitar a exclusão de uma trilha após o fechamento de uma Conta da AWS, consulte [Conta da AWS encerramento e trilhas](#) no Guia do CloudTrail usuário.

Como encerrar uma conta

Você pode fechar o seu Conta da AWS usando o procedimento a seguir. Observe que há orientações diferentes fornecidas em cada guia, dependendo do tipo de conta [autônoma, membro, gerencial e AWS GovCloud (US)] que você deseja fechar.

Se você tiver algum problema durante o processo de encerramento da conta, consulte [Solução de problemas com Conta da AWS encerramento](#).

Standalone account

Uma conta autônoma é uma conta gerenciada individualmente que não faz parte da AWS Organizations.

Para encerrar uma conta autônoma na página Contas

1. [Faça login no Console de gerenciamento da AWS como usuário root](#) no Conta da AWS que você deseja fechar. Você não poderá encerrar uma conta se tiver feito login como usuário ou perfil do IAM.
2. No canto superior direito da barra de navegação, selecione o nome ou número da conta e, em seguida, selecione Conta.
3. Na página [Conta](#), escolha o botão Encerrar conta.
4. Digite o ID da conta (exibido na parte superior da caixa de diálogo de encerramento) para confirmar que você leu e entendeu o processo de encerramento da conta.
5. Escolha o botão Encerrar conta para iniciar o processo de encerramento da conta.
6. Em alguns minutos, você receberá uma confirmação por e-mail de que a conta foi encerrada.

Note

Essa tarefa não é compatível com AWS CLI ou por uma operação de API de um dos AWS SDKs. Você pode executar essa tarefa somente usando Console de gerenciamento da AWS o.

Member account

Uma conta de membro Conta da AWS faz parte de AWS Organizations.

Para fechar uma conta de membro a partir do AWS Organizations console

1. Faça login no [console do AWS Organizations](#).
2. Na página Contas da AWS, localize e escolha o nome da conta de membro que deseja encerrar. É possível navegar na hierarquia da UO ou ver uma lista simples de contas sem a estrutura da UO.
3. Escolha Fechar conta ao lado do nome da conta na parte superior da página. Essa opção só está disponível quando uma organização da AWS está no modo [Todos os atributos](#).

 Note

Se sua organização estiver usando o modo de [cobrança consolidada](#), você não poderá ver o botão Fechar conta no console. Para encerrar uma conta no modo de faturamento consolidado, entre na conta que você deseja encerrar como usuário-raiz. Na página Contas, clique o botão Encerrar conta, insira o ID da sua conta e clique o botão Encerrar conta.

4. Leia e certifique-se de que entendeu as orientações para o encerramento da conta.
5. Insira o ID da conta-membro e selecione Encerrar conta para iniciar o processo de encerramento da conta.

 Note

Qualquer conta-membro que você encerrar exibirá uma etiqueta CLOSED ao lado do nome da conta no console do AWS Organizations por até 90 dias após a data de encerramento original. Depois de 90 dias, a conta-membro não será mais exibida no console do AWS Organizations .

Para encerrar uma conta-membro na página Contas

Opcionalmente, você pode fechar uma conta de AWS membro diretamente da [página Conta](#) no Console de gerenciamento da AWS. Para obter orientações passo a passo, siga as instruções na guia Conta autônoma.

Essa opção não está disponível para contas de projetos que não têm um usuário root. Feche as contas do projeto a partir do AWS Organizations console.

Para fechar uma conta de membro usando AWS CLI SDKs

Para obter instruções sobre como fechar uma conta de membro usando os SDKs AWS CLI e, consulte [Fechar uma conta de membro em sua organização](#) no Guia do AWS Organizations usuário.

Management account

Uma conta de gerenciamento é Conta da AWS aquela que atua como conta principal ou raiz do AWS Organizations.

Note

Você não pode encerrar uma conta de gerenciamento diretamente no console do AWS Organizations .

Para encerrar uma conta de gerenciamento na página Contas

1. [Faça login Console de gerenciamento da AWS como usuário root da](#) conta de gerenciamento que você deseja fechar. Você não poderá encerrar uma conta se tiver feito login como usuário ou perfil do IAM.
2. Verifique se não há contas-membro ativas restantes em sua organização. Para fazer isso, acesse o [console do AWS Organizations](#) e verifique se todas as contas-membro estão mostrando Closed ao lado dos nomes das contas. Se você tiver uma conta-membro ainda ativa, precisará seguir as orientações de encerramento de conta fornecidas na guia Conta-membro antes de passar para a próxima etapa.
3. No canto superior direito da barra de navegação, selecione o nome ou número da conta e, em seguida, selecione Conta.
4. Na página [Conta](#), escolha o botão Encerrar conta.
5. Digite o ID da conta (exibido na parte superior da caixa de diálogo de encerramento) para confirmar que você leu e entendeu o processo de encerramento da conta.
6. Escolha o botão Encerrar conta para iniciar o processo de encerramento da conta.
7. Em alguns minutos, você receberá uma confirmação por e-mail de que a conta foi encerrada.

 Note

Essa tarefa não é compatível com AWS CLI ou por uma operação de API de um dos AWS SDKs. Você pode executar essa tarefa somente usando Console de gerenciamento da AWS o.

AWS GovCloud (US) account

Uma AWS GovCloud (US) conta está sempre vinculada a um único padrão Conta da AWS para fins de cobrança e pagamento.

Para fechar uma AWS GovCloud (US) conta

Se você tem uma Conta da AWS que está vinculada a uma AWS GovCloud (US) conta, você precisa fechar a conta padrão antes de fechar a AWS GovCloud (US) conta. Para obter mais detalhes, incluindo como fazer backup de dados e evitar AWS GovCloud (US) cobranças não intencionais, consulte [Fechar uma AWS GovCloud \(US\) conta](#) no Guia do AWS GovCloud (US) usuário.

O que esperar depois de encerrar a conta

Imediatamente após o encerramento da conta, ocorrerá o seguinte:

- Você receberá um e-mail confirmando o encerramento da conta no endereço de e-mail do usuário-raiz. Se você não receber esse e-mail em algumas horas, consulte [Solução de problemas com Conta da AWS encerramento](#).
- Qualquer conta de membro que você fechar exibirá uma CLOSED etiqueta ao lado do nome da conta no AWS Organizations console por até 90 dias após a data de encerramento original. Após 90 dias, a conta do membro não será mais exibida no AWS Organizations console.
- Se você concedeu permissões para acessar serviços em suas Conta da AWS duas outras contas, qualquer solicitação de acesso feita a partir dessas contas deverá falhar após o encerramento da conta. Se você reabrir sua Conta da AWS, outras pessoas Contas da AWS poderão acessar novamente os AWS serviços e recursos da sua conta se você conceder as permissões necessárias a elas.

O encerramento da conta pode não ocorrer imediatamente em todas as regiões e serviços e pode levar várias horas para ser concluído.

Post-closure período

O período pós-fechamento se refere ao período de tempo entre o dia em que você fechou sua conta e o momento em que fecha AWS permanentemente sua. Conta da AWS O período pós-encerramento é de 90 dias. Durante o período pós-encerramento, você só poderá acessar o conteúdo e os serviços da AWS se reabrir a conta. Após o período pós-fechamento, fecha AWS permanentemente o seu Conta da AWS e você não poderá mais reabri-lo. AWS também excluirá conteúdo e recursos da sua conta (exceto CloudTrail trilhas). Depois que uma conta tiver sido encerrada permanentemente, o [ID da Conta da AWS](#) nunca poderá ser reutilizado.

Reabrindo seu Conta da AWS

Sua conta será encerrada permanentemente em 90 dias, após os quais você não poderá reabrir sua conta e AWS excluirá o conteúdo restante em sua conta. Para reabrir sua conta antes que ela seja encerrada permanentemente, consulte [Reabrir um Conta da AWS](#).

Note

As cobranças pelos serviços que permaneceram na conta serão reiniciadas se você reabri-la.

Reabrir um Conta da AWS

Se você fechou o seu Conta da AWS e não tem um saldo pendente, você mesmo pode reabri-lo durante o período [pós-fechamento](#).

Você reabre sua conta fazendo login como usuário root e enviando a solicitação na página Contas.

O que você precisa saber antes de reabrir sua conta

Antes de reabrir seu Conta da AWS, observe o seguinte:

- Self-service requisitos: Você pode usar esse processo de autoatendimento somente se você mesmo tiver fechado a conta e se sua conta não tiver saldo pendente no momento do encerramento da conta. Você deve fazer login como usuário raiz da conta fechada; você não pode

reabrir uma conta enquanto estiver conectado como usuário ou função do IAM. Você deve enviar sua solicitação de reabertura dentro de 90 dias após o fechamento da conta, durante o período pós-encerramento.

- Contas fechadas por AWS: Se sua conta AWS foi fechada, você não poderá reabri-la sozinho. Pague qualquer saldo pendente dentro de 30 dias a partir da data em que sua conta foi encerrada e entre em contato [AWS Support](#) para reabrir sua conta.
- Pagamentos e cobranças: sua conta deve ter uma forma de pagamento válida e não expirada. Como a fatura do mês anterior é finalizada no início do mês seguinte, você pode ter um saldo pendente para uso antes do fechamento, mesmo que sua conta não tivesse saldo no encerramento. Para revisar ou pagar um saldo, consulte Como [fazer pagamentos](#). Quando você reabre sua conta, as cobranças são retomadas por quaisquer serviços ainda em execução nela. Se você não interrompeu esses serviços antes de fechar a conta, também pode ter incorrido em cobranças durante o período pós-encerramento.

Como reabrir sua conta

Siga estas etapas para reabrir sua conta fechada.

Note

Essa tarefa não é compatível com AWS CLI ou por uma operação de API de um dos AWS SDKs. Você pode executar essa tarefa somente usando Console de gerenciamento da AWS o.

Para reabrir sua conta na página Contas

1. [Faça login no Console de gerenciamento da AWS como usuário root do](#) fechado Conta da AWS que você deseja reabrir. Você não pode reabrir uma conta enquanto estiver conectado como usuário ou função do IAM.
2. Abra a página Contas da conta fechada, da seguinte forma: No banner da conta fechada, escolha Reabrir conta.
3. Na caixa de diálogo Reabrir conta, insira o ID da conta mostrado na caixa de diálogo para confirmar que você deseja reabrir a conta.
4. Escolha Reabrir conta para enviar sua solicitação. Uma mensagem confirma que a reabertura da conta foi iniciada.

5. Aguarde a conclusão da reabertura. Quando sua conta estiver ativa novamente, uma mensagem confirma que a conta foi reaberta com sucesso e que seus AWS serviços e faturamento foram restaurados.

Se não AWS conseguir reabrir sua conta, você receberá uma notificação do console explicando por que e como resolver o problema.

O que esperar depois de reabrir sua conta

Depois de enviar uma solicitação de reabertura, ocorre o seguinte:

- Para verificar o status, atualize a página Contas. Quando a reabertura for concluída, a conta será exibida como ativa e o banner da conta fechada não aparecerá mais.
- Depois que a conta estiver ativa, AWS restaura o acesso aos serviços e recursos e o faturamento é retomado.

Prepare sua conta para uso após a reabertura

Alguns recursos e assinaturas não são restaurados automaticamente para o estado de execução. Depois que sua conta for reaberta, talvez seja necessário fazer o seguinte antes de retomar as operações normais:

- Inicie todas as instâncias do Amazon EC2 que foram interrompidas no encerramento da conta. Para obter mais informações, consulte [Iniciar uma instância](#) no Guia do usuário do Amazon EC2.
- Restaure os bancos de dados do Amazon RDS a partir dos snapshots criados no encerramento da conta.
- Cancele e assine novamente todas as AWS Marketplace assinaturas. As assinaturas não são restauradas automaticamente na reabertura da conta.

Disponibilidade de regiões

Self-service a reabertura da conta está disponível em todas as regiões comerciais.

Segurança em AWS Gerenciamento de contas

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 serviços no Nuvem AWS. 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 Conformidade Programas de [AWS](#). Para saber mais sobre os programas de conformidade que se aplicam ao gerenciamento de contas, consulte [Serviços da AWS escopo por programa](#).
- **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 empresa e as leis e regulamentos aplicáveis.

O modelo de responsabilidade compartilhada é aplicado a todos Contas da AWS. Isso inclui Contas da AWS criar usando nossa nova AWS experiência e contas criadas usando nossa AWS experiência avançada.

Esta documentação ajuda você a entender como aplicar o modelo de responsabilidade compartilhada ao usar o Gerenciamento de AWS contas. Ela mostra como configurar o Gerenciamento de Contas para atender aos objetivos de segurança e conformidade. Você também aprenderá a usar outros AWS serviços que ajudam você a monitorar e proteger seus recursos de gerenciamento de contas. Parte dessa documentação só é relevante para contas criadas com nossa AWS experiência avançada. Identificaremos quando a documentação só é relevante para contas criadas com nossa AWS experiência avançada.

Tópicos

- [Proteção de dados em AWS Gerenciamento de contas](#)
- [AWS PrivateLink for AWS Gerenciamento de contas](#)
- [Identity and Access Management para AWS Gerenciamento de contas](#)

- [AWS políticas gerenciadas para AWS Gerenciamento de contas](#)
- [Validação de conformidade AWS Gerenciamento de contas](#)
- [Resiliência em AWS Gerenciamento de contas](#)
- [Segurança de infraestrutura em AWS Gerenciamento de contas](#)

Proteção de dados em AWS Gerenciamento de contas

As informações a seguir são relevantes para todos Contas da AWS.

O modelo de responsabilidade AWS <https://aws.amazon.com/compliance/shared-responsibility-model/> se aplica à proteção de dados no gerenciamento de AWS contas. 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 gerenciamento de contas ou outros 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.

AWS PrivateLink for AWS Gerenciamento de contas

As informações a seguir são relevantes para todos Contas da AWS.

Se você usa o Amazon Virtual Private Cloud (Amazon VPC) para hospedar seus AWS recursos, você pode acessar o serviço de gerenciamento de AWS contas de dentro da VPC sem precisar atravessar a Internet pública.

O Amazon VPC permite que você inicie AWS recursos em uma rede virtual personalizada. Você pode usar uma VPC para controlar as configurações de rede, como o intervalo de endereços IP, sub-redes, tabelas de rotas e gateways de rede. Para obter informações sobre como criar suas próprias VPCs, consulte o [Guia do usuário da Amazon VPC](#).

Para conectar a Amazon VPC ao Gerenciamento de Contas, primeiro você deve definir um endpoint da VPC de interface, que permite conectar a VPC a outros produtos da AWS . O endpoint fornece conectividade confiável e escalável sem a necessidade de um gateway da internet, da instância de conversão de endereço de rede (NAT) ou de uma conexão VPN. Para obter mais informações, consulte [Endpoints da VPC da interface \(AWS PrivateLink\)](#) no Guia do usuário da Amazon VPC.

Criação do endpoint

Você pode criar um endpoint de gerenciamento de AWS contas em sua VPC usando o AWS Command Line Interface (AWS CLI) Console de gerenciamento da AWS, um AWS SDK, a API de gerenciamento de AWS contas ou. CloudFormation

Para obter informações sobre como criar e configurar um endpoint usando o console do Amazon VPC ou o AWS CLI, consulte [Criação de um endpoint de interface](#) no Guia do usuário do Amazon VPC.

Note

Ao criar um endpoint, especifique o Gerenciamento de Contas como o serviço ao qual a VPC deve se conectar, usando o seguinte formato:

```
com.amazonaws.us-east-1.account
```

Você deve usar a string exatamente como mostrada, especificando a região `us-east-1`. Como um serviço global, o gerenciamento de contas é hospedado somente nessa AWS região.

Para obter informações sobre como criar e configurar um endpoint usando CloudFormation, consulte o recurso [AWS: :EC2: :VPCendpoint](#) no Guia do usuário. CloudFormation

Políticas de endpoint da Amazon VPC

Você pode controlar quais ações podem ser executadas por meio desse endpoint de serviço anexando uma política de endpoint ao criar o endpoint Amazon VPC. É possível criar regras complexas do IAM anexando várias políticas de endpoint. Para obter mais informações, consulte:

- [Políticas de endpoint da Amazon Virtual Private Cloud para o Gerenciamento de Contas](#)
- [Controle do acesso a serviços com endpoints da VPC](#) no Guia do AWS PrivateLink .

Políticas de endpoint da Amazon Virtual Private Cloud para o Gerenciamento de Contas

As informações a seguir são relevantes para todos Contas da AWS.

Você pode criar uma política de endpoint da Amazon VPC para o Gerenciamento de Contas, na qual você especifica o seguinte:

- A entidade principal que pode realizar ações.
- As ações que as entidades principais podem executar.
- Os recursos nos quais as ações podem ser executadas.

O exemplo a seguir mostra uma política de endpoint do Amazon VPC que permite que um usuário do IAM chamado Alice na conta 123456789012 recupere e altere as informações de contato alternativas de qualquer conta da AWS, mas nega a todos os usuários do IAM a permissão de excluir qualquer informação de contato alternativa em qualquer conta.

Se você quiser conceder acesso às contas que fazem parte de uma AWS organização a um diretor que esteja em uma das contas membros da organização, o Resource element deverá usar o seguinte formato:

```
arn:aws:account::{ManagementAccountId}:account/o-{OrganizationId}/{AccountId}
```

Para obter mais informações sobre a criação de políticas de endpoint, consulte [Controle do acesso a serviços com endpoints da VPC](#) no Guia do AWS PrivateLink .

Identity and Access Management para AWS Gerenciamento de contas

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 (ter permissões) para usar os recursos do Gerenciamento de Contas. O IAM é um AWS service (Serviço da AWS) que você pode usar sem custo adicional.

As informações a seguir são sobre Identity and Access Management for AWS Account Management. Essas informações são mais relevantes para Contas da AWS aquelas que você cria quando usa nossa AWS experiência avançada ou se ativou recursos avançados para sua conta. Para saber como o controle de acesso funciona em nossa nova AWS experiência, consulte [Compare o gerenciamento de acesso](#).

Tópicos

- [Público](#)
- [Autenticação com identidades](#)
- [Gerenciar o acesso usando políticas](#)
- [Como AWS O gerenciamento de contas funciona com o IAM](#)
- [Identity-based exemplos de políticas para AWS Gerenciamento de contas](#)

- [Usando políticas baseadas em identidade \(políticas do IAM\) para AWS Gerenciamento de contas](#)
- [Solução de problemas AWS Identidade e acesso ao gerenciamento de contas](#)

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 AWS Identidade e acesso ao gerenciamento de contas](#)).
- Administrador do serviço: determine o acesso do usuário e envie solicitações de permissão (consulte [Como AWS O gerenciamento de contas funciona com o IAM](#))
- Administrador do IAM: escreva políticas para gerenciar o acesso (consulte [Identity-based exemplos de políticas para AWS Gerenciamento de contas](#))

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 AWS O gerenciamento de contas funciona com o IAM

Essas informações são mais relevantes para Contas da AWS as que você cria ao usar nossa AWS experiência avançada. Para saber como o controle de acesso funciona em nossa nova AWS experiência, consulte [Compare o gerenciamento de acesso](#).

Antes de usar o IAM para gerenciar o acesso ao Gerenciamento de Contas, saiba quais recursos do IAM estão disponíveis para uso com o Gerenciamento de Contas.

Recursos do IAM que você pode usar com AWS Gerenciamento de contas

Recurso do IAM	Suporte ao Gerenciamento de Contas
Identity-based políticas	Sim
Resource-based políticas	Não

Recurso do IAM	Suporte ao Gerenciamento de Contas
Ações de políticas	Sim
Recursos de políticas	Sim
Chaves de condição de políticas	Sim
ACLs	Não
ABAC (tags em políticas)	Não
Credenciais temporárias	Sim
Permissões de entidade principal	Sim
Perfis de serviço	Não
Service-linked funções	Não

Para ter uma visão de alto nível de como o gerenciamento de contas 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 gerenciamento de contas

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 gerenciamento de contas

Para visualizar exemplos de políticas baseadas em identidade de Gerenciamento de Contas, consulte [Identity-based exemplos de políticas para AWS Gerenciamento de contas](#).

Resource-based políticas dentro do gerenciamento de contas

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 de política para Gerenciamento de Contas

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 ações de gerenciamento de contas, consulte [Ações definidas pelo gerenciamento de AWS contas](#) na Referência de autorização de serviço.

As ações de política no Gerenciamento de Contas usam o prefixo a seguir antes da ação.

```
account
```

Para especificar várias ações em uma única instrução, separe-as com vírgulas.

```
"Action": [
```

```
"account:action1",  
"account:action2"  
]
```

Você também pode especificar várias ações usando caracteres-curinga (*). Por exemplo, para especificar todas as ações que funcionam com os contatos alternativos Conta da AWS de um, inclua a ação a seguir.

```
"Action": "account:*AlternateContact"
```

Para visualizar exemplos de políticas baseadas em identidade de Gerenciamento de Contas, consulte [Identity-based exemplos de políticas para AWS Gerenciamento de contas](#).

Recursos de políticas para Gerenciamento de Contas

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": "*" 
```

O serviço de gerenciamento de contas oferece suporte aos seguintes tipos de recursos específicos em um `Resource` elemento de política do IAM para ajudar você a filtrar a política e distinguir entre esses tipos de Contas da AWS:

- `account`

Esse tipo de `resource` corresponde apenas a Contas da AWS autônomas que não são contas-membro em uma organização gerenciada pelo serviço do AWS Organizations .

- `accountInOrganization`

Esse `resource` tipo corresponde apenas Contas da AWS às contas de membros em uma organização gerenciada pelo AWS Organizations serviço.

Para ver uma lista dos tipos de recursos de gerenciamento de contas e seus ARNs, consulte [Recursos definidos pelo gerenciamento de AWS contas](#) na Referência de autorização de serviço. Para saber com quais ações você pode especificar o ARN de cada recurso, consulte [Ações definidas pelo gerenciamento de AWS contas](#).

Para visualizar exemplos de políticas baseadas em identidade de Gerenciamento de Contas, consulte [Identity-based exemplos de políticas para AWS Gerenciamento de contas](#).

Chaves de condição de política Gerenciamento de Contas

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.

O serviço de Gerenciamento de Contas oferece suporte às seguintes chaves de condição que você pode usar para fornecer filtragem refinada para as políticas do IAM:

- `conta: TargetRegion`

Essa chave de condição usa um argumento que consiste em uma lista de [códigos de região da AWS](#). Ela permite filtrar a política para afetar somente as ações que se aplicam às regiões especificadas.

- `conta: AlternateContactTypes`

Essa chave de condição usa uma lista de tipos de contato alternativos:

- BILLING
- OPERATIONS
- SECURITY

O uso dessa chave permite filtrar a solicitação somente para as ações direcionadas aos tipos de contato alternativos especificados.

- `conta: AccountResourceOrgPaths`

Essa chave de condição usa um argumento que consiste em uma lista de caminhos na hierarquia de sua organização para unidades organizacionais (UO) específicas. Ela permite que você filtre a política para afetar somente contas de destino em uma UO correspondente.

```
o-aa111bb222/r-a1b2/ou-a1b2-f6g7h111/*
```

- conta: AccountResourceOrgTags

Essa chave de condição usa um argumento que consiste em uma lista de chaves e valores de tag. Ela permite que você filtre a política para afetar somente as contas que são membros de uma organização e que estão marcadas com as chaves e valores de tag especificados.

- conta: EmailTargetDomain

Essa chave de condição usa um argumento que consiste em uma lista de domínios de e-mail. Ela permite filtrar a política para afetar somente as ações que correspondem aos domínios de e-mail especificados. Essa chave de condição diferencia maiúsculas de minúsculas. Você deve usar `StringEqualsIgnoreCase` em vez de `StringEquals` no bloco de condição da política para controlar a ação com base no domínio do endereço de e-mail de destino. Aqui está um exemplo de política que permite que a ação `account:StartPrimaryEmailUpdate` seja concluída quando o domínio de e-mail contém `example.com`, `company.org` ou qualquer combinação de maiúsculas e minúsculas, como `EXAMPLE.COM`.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowConditionKey",
      "Effect": "Allow",
      "Action": [
        "account:StartPrimaryEmailUpdate"
      ],
      "Resource": "*",
      "Condition": {
        "StringEqualsIgnoreCase": {
          "account:EmailTargetDomain": [
            "example.com",
            "company.org"
          ]
        }
      }
    }
  ]
}
```

```
}  
  ]  
}
```

Para ver uma lista das chaves de condição de gerenciamento de contas, consulte [Chaves de condição para gerenciamento de AWS contas](#) na Referência de autorização de serviço. Para saber com quais ações e recursos você pode usar uma chave de condição, consulte [Ações definidas pelo gerenciamento de AWS contas](#).

Para visualizar exemplos de políticas baseadas em identidade de Gerenciamento de Contas, consulte [Identity-based exemplos de políticas para AWS Gerenciamento de contas](#).

Listas de controle de acesso em Gerenciamento de Contas

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 com gerenciamento de contas

Oferece compatibilidade com ABAC (tags em políticas): não

Attribute-based controle de acesso (ABAC) é uma estratégia de autorização que define permissões com base em atributos. Em AWS, esses atributos são chamados de tags. Você pode anexar tags a entidades do IAM (usuários ou funções) e a vários AWS recursos. Marcar de entidades e atributos é a primeira etapa do ABAC. Em seguida, você cria políticas de ABAC para permitir operações quando a tag da entidade principal corresponder à tag do recurso que ela estiver tentando acessar.

O ABAC é útil em ambientes que estão crescendo rapidamente e ajuda em situações em que o gerenciamento de políticas se torna um problema.

Para o gerenciamento de AWS contas, o controle de acesso baseado em tags é suportado somente por meio da chave de `account:AccountResourceOrgTags/key-name` condição. A chave de condição `aws:ResourceTag/key-name` padrão não é compatível com APIs no namespace da conta.

Exemplo de política JSON usando a chave de condição compatível

O exemplo de política a seguir permite acessar as informações de contato de contas marcadas com a chave "CostCenter" e o valor "12345" ou "67890" em sua organização.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "account:GetContactInformation",
        "account:GetAlternateContact"
      ],
      "Resource": "*",
      "Condition": {
        "ForAnyValue:StringEquals": {
          "account:AccountResourceOrgTags/CostCenter": [
            "12345",
            "67890"
          ]
        }
      }
    }
  ]
}
```

Para obter mais informações sobre o ABAC, consulte [Definir permissões com base em atributos com autorização ABAC](#) e o [tutorial do IAM: Definir permissões para acessar AWS recursos com base em tags no Guia](#) do usuário do IAM.

Usar credenciais temporárias com o Gerenciamento de Contas

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 gerenciamento de contas

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](#).

Perfis de serviço para o Gerenciamento de Contas

Compatível com perfis de serviço: não

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.

Service-linked funções para gerenciamento de contas

Compatível com perfis vinculados ao serviço: Não

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 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 AWS Gerenciamento de contas

Essas informações são mais relevantes para Contas da AWS as que você cria ao usar nossa AWS experiência avançada. Para saber como o controle de acesso funciona em nossa nova AWS experiência, consulte [Compare o gerenciamento de acesso](#).

Por padrão, usuários e perfis não têm permissão para criar ou modificar recursos do Gerenciamento de Contas. 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 pelo Gerenciamento de contas, incluindo o formato dos ARNs para cada um dos tipos de recursos, consulte [Ações, recursos e chaves de condição para gerenciamento de AWS contas](#) na Referência de autorização de serviço.

Tópicos

- [Práticas recomendadas de política](#)
- [Usando a página Conta no Console de gerenciamento da AWS](#)
- [Fornecendo acesso somente para leitura à página Conta no Console de gerenciamento da AWS](#)
- [Fornecendo acesso total à página Conta no Console de gerenciamento da AWS](#)

Práticas recomendadas de política

Identity-based as políticas determinam se alguém pode criar, acessar ou excluir recursos de gerenciamento de contas 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 a página Conta no Console de gerenciamento da AWS

Para acessar a [página Conta](#) no Console de gerenciamento da AWS, você deve ter um conjunto mínimo de permissões. Essas permissões devem permitir que você liste e visualize detalhes sobre seu Conta da AWS. Se você criar uma política baseada em identidade que seja mais restritiva que as permissões mínimas necessárias, o console não funcionará como pretendido para entidades (usuários ou perfis do IAM) com essa política.

Para garantir que usuários e funções possam usar o console de gerenciamento de contas, você pode optar por anexar a política `AWSAccountManagementReadOnlyAccess` ou a política `AWSAccountManagementFullAccess` AWS gerenciada às entidades. Para saber mais, consulte [Adicionar permissões a um usuário](#) no Guia do usuário do IAM.

Você não precisa permitir permissões mínimas do console para usuários que estão fazendo chamadas somente para a AWS CLI ou a AWS API. Em vez disso, em muitos casos, você pode optar por permitir o acesso somente às ações que correspondem às operações de API que você está tentando realizar.

Fornecendo acesso somente para leitura à página Conta no Console de gerenciamento da AWS

No exemplo a seguir, você deseja conceder a um usuário do IAM na Conta da AWS acesso somente leitura à página Conta no Console de gerenciamento da AWS. Usuários com essa política anexada não podem fazer qualquer alteração.

A ação `account:GetAccountInformation` concede acesso para a visualização da maioria das configurações na página Conta. No entanto, para visualizar as regiões AWS atualmente habilitadas, você também deve incluir a ação `account:ListRegions`.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "GrantReadOnlyAccessToAccountSettings",
      "Effect": "Allow",
      "Action": [
        "account:GetAccountInformation",
        "account:ListRegions"
      ],
      "Resource": "*"
    }
  ]
}
```

Fornecendo acesso total à página Conta no Console de gerenciamento da AWS

No exemplo a seguir, você deseja conceder a um usuário do IAM na Conta da AWS acesso total à página Conta no Console de gerenciamento da AWS. Usuários com essa política anexada podem alterar as configurações da conta.

Esse exemplo de política se baseia no exemplo anterior, adicionando cada uma das permissões de gravação disponíveis (com exceção de `CloseAccount`), o que permite ao usuário alterar a maioria das configurações da conta, incluindo as permissões `account:EnableRegion` e `account:DisableRegion`.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "GrantFullAccessToAccountSettings",
      "Effect": "Allow",
      "Action": [
        "account:GetAccountInformation",
        "account:ListRegions",
        "account:PutContactInformation",
        "account:PutAlternateContact",
        "account>DeleteAlternateContact",
        "account:EnableRegion",
        "account:DisableRegion"
      ],
      "Resource": "*"
    }
  ]
}
```

Usando políticas baseadas em identidade (políticas do IAM) para AWS Gerenciamento de contas

Essas informações são mais relevantes para Contas da AWS as que você cria ao usar nossa AWS experiência avançada. Para saber como o controle de acesso funciona em nossa nova AWS experiência, consulte [Compare o gerenciamento de acesso](#).

Para uma discussão completa sobre usuários Contas da AWS e usuários do IAM, consulte [O que é o IAM?](#) no Guia do usuário do IAM.

Para obter instruções sobre como atualizar as políticas gerenciadas pelo cliente, consulte [Editar políticas do IAM](#) no Guia do usuário do IAM.

AWS Políticas de ações de gerenciamento de contas

Esta tabela resume as permissões que concedem acesso às configurações da conta. Para obter exemplos de políticas que usam essas permissões, consulte [Identity-based exemplos de políticas para AWS Gerenciamento de contas](#).

 Note

Para conceder aos usuários do IAM acesso de gravação a uma configuração de [conta específica na página Conta](#) do Console de gerenciamento da AWS, você deve conceder a `GetAccountInformation` permissão, além da permissão (ou permissões) que deseja usar para modificar essa configuração.

Nome da permissão	Nível de acesso	Description
<code>account:ListRegions</code>	Lista	Concede permissão para listar as regiões disponíveis.
<code>account:GetAccountInformation</code>	Ler	Concede permissão para recuperar as informações de uma conta.
<code>account:GetAlternateContact</code>	Ler	Concede permissão para recuperar os contatos alternativos de uma conta.
<code>account:GetContactInformation</code>	Ler	Concede permissão para recuperar as informações do contato principal de uma conta.
<code>account:GetPrimaryEmail</code>	Ler	Concede permissão para recuperar o endereço de e-mail principal de uma conta.
<code>account:GetRegionOptStatus</code>	Ler	Concede permissão para obter o status de ativação de uma região.
<code>account:AcceptPrimaryEmailUpdate</code>	Gravar	Concede permissão para aceitar a atualização do endereço de e-mail principal

Nome da permissão	Nível de acesso	Description
		da conta do membro em uma AWS organização.
<code>account:CloseAccount</code>	Gravar	<p>Concede permissão para fechar uma conta.</p> <div>  Note Esta é uma permissão somente para o console. Não há acesso de API disponível para esta permissão. </div>
<code>account:DeleteAlternateContact</code>	Gravar	Concede permissão para excluir os contatos alternativos de uma conta.
<code>account:DisableRegion</code>	Gravar	Concede permissão para desabilitar o uso de uma região.
<code>account:EnableRegion</code>	Gravar	Concede permissão para habilitar o uso de uma região.
<code>account:PutAccountName</code>	Gravar	Concede permissão para atualizar o nome de um conta.
<code>account:PutAlternateContact</code>	Gravar	Concede permissão para modificar os contatos alternativos de uma conta.

Nome da permissão	Nível de acesso	Description
<code>account:PutContactInformation</code>	Gravar	Concede permissão para atualizar as informações do contato principal de uma conta.
<code>account:SendPhoneNumberVerification</code>	Gravar	Concede permissão para enviar um código de verificação para o número de telefone de contato principal de uma conta.
<code>account:StartPrimaryEmailUpdate</code>	Gravar	Concede permissão para iniciar a atualização do endereço de e-mail principal da conta do membro em uma AWS organização.
<code>account:VerifyPhoneNumber</code>	Gravar	Concede permissão para verificar o número de telefone de contato principal de uma conta enviando um código de verificação.

Solução de problemas AWS Identidade e acesso ao gerenciamento de contas

Essas informações são mais relevantes para Contas da AWS as que você cria ao usar nossa AWS experiência avançada. Para saber como o controle de acesso funciona em nossa nova AWS experiência, consulte [Compare o gerenciamento de acesso](#).

Use as informações a seguir para ajudar no diagnóstico e na correção de problemas comuns que você pode encontrar quando trabalhar com o Gerenciamento de Contas e o IAM.

Tópicos

- [Não tenho autorização para executar uma ação na página Contas](#)

- [Não estou autorizado a realizar iam: PassRole](#)
- [Quero permitir que pessoas fora da minha Conta da AWS para acessar os detalhes da minha conta](#)

Não tenho autorização para executar uma ação na página Contas

Se o Console de gerenciamento da AWS indicar que você não está autorizado a realizar uma ação, entre em contato com o administrador para obter ajuda. O administrador é a pessoa que forneceu o seu nome de usuário e senha.

O exemplo de erro a seguir ocorre quando o usuário do mateojackson IAM tenta usar o console para ver detalhes sobre ele Conta da AWS na página Conta do Console de gerenciamento da AWS, mas não tem as `account:GetAccountInformation` permissões.

**You Need Permissions**

You don't have permission to access billing information for this account. Contact your AWS administrator if you need help. If you are an AWS administrator, you can provide permissions for your users or groups by making sure that (1) [this account allows IAM and federated users to access billing information](#) and (2) [you have the required IAM permissions](#).

Neste caso, Mateo pede ao administrador para atualizar suas políticas para permitir a ele o acesso ao recurso *my-example-widget* usando a ação `account:GetWidget`.

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 políticas deverão ser atualizadas para permitir a passagem de um perfil para o Gerenciamento de Contas.

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 fazer isso, é preciso ter permissões para passar o perfil para o serviço.

O exemplo de erro a seguir ocorre quando uma usuária do IAM chamada `marymajor` tenta usar o console para executar uma ação no Gerenciamento de Contas. 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 os detalhes da minha conta

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 o Gerenciamento de Contas é compatível com esses recursos, consulte [Como AWS O gerenciamento de contas funciona 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.

AWS políticas gerenciadas para AWS Gerenciamento de contas

Essas informações são mais relevantes para as Contas da AWS que você cria ao usar nossa AWS experiência avançada ou ao ativar recursos avançados para sua conta. Para saber como o controle de acesso funciona em nossa nova AWS experiência, consulte [Compare o gerenciamento de acesso](#).

AWS Atualmente, o gerenciamento de contas fornece duas políticas AWS gerenciadas que estão disponíveis para seu uso:

- [AWS política gerenciada: AWSAccountManagementReadOnlyAccess](#)
- [AWS política gerenciada: AWSAccountManagementFullAccess](#)
- [Atualizações do gerenciamento de contas para AWS políticas gerenciadas](#)

Uma política AWS gerenciada é uma política independente criada e administrada por AWS. AWS as políticas gerenciadas são projetadas para fornecer permissões para muitos casos de uso comuns, para que você possa começar a atribuir permissões a usuários, grupos e funções.

Lembre-se de que as políticas AWS gerenciadas podem não conceder permissões de menor privilégio para seus casos de uso específicos, pois elas estão disponíveis para uso de todos os AWS clientes. Recomendamos que você reduza ainda mais as permissões definindo as [políticas gerenciadas pelo cliente](#) que são específicas para seus casos de uso.

Você não pode alterar as permissões definidas nas políticas AWS gerenciadas. Se AWS atualizar as permissões definidas em uma política AWS gerenciada, a atualização afetará todas as identidades principais (usuários, grupos e funções) às quais a política está anexada. AWS é mais provável que atualize uma política AWS gerenciada quando uma nova AWS service (Serviço da AWS) é lançada ou quando novas operações de API são disponibilizadas para os serviços existentes.

Para saber mais, consulte [AWS Políticas gerenciadas pela](#) no Guia do usuário do IAM.

AWS política gerenciada: AWSAccountManagementReadOnlyAccess

É possível anexar a política AWSAccountManagementReadOnlyAccess às suas identidades do IAM.

Essa política fornece permissões somente leitura para a visualização apenas do seguinte:

- Os metadados sobre seu Contas da AWS
- Os Regiões da AWS que estão ativados ou desativados para o Conta da AWS (você pode ver o status das regiões em sua conta somente usando o AWS console)

Ele faz isso concedendo permissão para executar qualquer uma das operações `Get*` ou `List*`. Ele não permite modificar os metadados da conta nem ativar ou desativar Regiões da AWS a conta.

Detalhes das permissões

Esta política inclui as seguintes permissões.

- **account**— Permite que os diretores recuperem as informações de metadados sobre. Contas da AWS Também permite que as entidades principais listem as Regiões da AWS que estão habilitadas para a conta no Console de gerenciamento da AWS.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "account:Get*",
        "account:List*"
      ],
      "Resource": "*"
    }
  ]
}
```

AWS política gerenciada: AWSAccountManagementFullAccess

É possível anexar a política `AWSAccountManagementFullAccess` às suas identidades do IAM.

Essa política fornece acesso administrativo total para a visualização ou a modificação do seguinte:

- Os metadados sobre seu Contas da AWS
- Os Regiões da AWS que estão ativados ou desativados para o Conta da AWS (você pode visualizar o status ou ativar ou desativar regiões da sua conta somente usando o AWS console)

Ele faz isso concedendo permissão para executar qualquer operação `account`.

Detalhes das permissões

Esta política inclui as seguintes permissões.

- **account**— Permite que os diretores visualizem ou modifiquem as informações de metadados sobre. Contas da AWS Também permite que as entidades principais listem as Regiões da AWS

que estão habilitadas para a conta e as habilitem ou desabilitem no Console de gerenciamento da AWS.

JSON

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

Atualizações do gerenciamento de contas para AWS políticas gerenciadas

Veja detalhes sobre atualizações nas políticas AWS gerenciadas de gerenciamento de contas desde que esse serviço começou a rastrear essas alterações. Para receber alertas automáticos sobre alterações nesta página, assine o feed de RSS na página Histórico do documento do Gerenciamento de Contas.

Alteração	Descrição	Data
AWS O gerenciamento de contas foi lançado com novas políticas AWS gerenciadas e começou a monitorar as mudanças	O gerenciamento de contas foi lançado inicialmente com as seguintes políticas AWS gerenciadas: <ul style="list-style-type: none">• AWSAccountManagemementReadOnlyAccess• AWSAccountManagemementFullAccess	30 de setembro de 2021

Validação de conformidade AWS Gerenciamento de contas

Nossa nova AWS experiência não pode ser usada para nenhuma carga de trabalho regulamentada. As informações a seguir são relevantes apenas para contas criadas quando você usa o Sign up for AWS (avançado).

Third-party os auditores avaliam a segurança e a conformidade dos AWS serviços que podem ser executados em sua empresa Conta da AWS como parte de vários programas de AWS conformidade. Isso inclui SOC, PCI, FedRAMP, HIPAA e outros.

Para obter uma lista de AWS serviços no escopo de programas de conformidade específicos, consulte [Serviços da AWS em escopo por programa de conformidade](#). 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](#) no Guia AWS Artifact do usuário.

Sua responsabilidade de conformidade ao usar seus serviços Conta da AWS é determinada pela confidencialidade de seus dados, pelos objetivos de conformidade da sua empresa e pelas leis e regulamentações aplicáveis. AWS fornece os seguintes recursos para ajudar na conformidade:

- [Guias de início rápido de segurança e conformidade](#) — Esses guias de implantação discutem considerações arquitetônicas e fornecem etapas para a implantação de ambientes básicos AWS focados na segurança e na conformidade.
- [Arquitetura para segurança e conformidade com a HIPAA na Amazon Web Services](#) — Este whitepaper descreve como as empresas podem usar para criar aplicativos. AWS HIPAA-eligible

Note

Nem todos Serviços da AWS são elegíveis para a HIPAA. Para obter mais informações, consulte a [Referência dos serviços qualificados pela HIPAA](#).

- [AWS Recursos de](#) — Esta coleção de pastas de trabalho e guias pode se aplicar ao seu setor e local.
- [Avaliação de recursos com regras](#) no Guia do AWS Config desenvolvedor — O AWS Config serviço avalia se suas configurações de recursos estão em conformidade com as práticas internas, as diretrizes do setor e as regulamentações.

- [AWS Security Hub CSPM](#)— Isso AWS service (Serviço da AWS) fornece uma visão abrangente do seu estado de segurança interno, AWS que ajuda você a verificar sua conformidade com os padrões e as melhores práticas do setor de segurança.
- [AWS Audit Manager](#)— Isso AWS service (Serviço da AWS) ajuda você a auditar continuamente seu AWS uso para simplificar o gerenciamento de riscos e a conformidade com regulamentos e padrões do setor.

Resiliência em AWS Gerenciamento de contas

As informações a seguir são relevantes para todos Contas da AWS. Se você usar nossa nova AWS experiência, considerações regionais adicionais se aplicam. Para obter mais informações, consulte [Regiões da AWS para seus projetos](#).

A infraestrutura AWS global é construída em torno Regiões da AWS de 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 zonas de disponibilidade Regiões da AWS e zonas de disponibilidade, consulte Infraestrutura [AWS global](#).

Segurança de infraestrutura em AWS Gerenciamento de contas

As informações a seguir são relevantes para todos Contas da AWS.

Como serviços gerenciados, AWS os serviços em execução no seu Conta da AWS são protegidos pela segurança de rede AWS global. Para obter informações sobre serviços AWS de segurança e como AWS protege a infraestrutura, consulte Segurança [AWS na nuvem](#). Para projetar seu AWS ambiente usando as melhores práticas de segurança de infraestrutura, consulte [Proteção de infraestrutura](#) no pilar de segurança AWS Well-Architected Framework.

Você usa chamadas de API AWS publicadas para acessar as configurações da conta 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.

Além disso, as solicitações devem ser assinadas usando um ID da chave de acesso e uma chave de acesso secreta associada a uma entidade principal do IAM. Ou você pode usar o [AWS Security Token Service](#) (AWS STS) para gerar credenciais de segurança temporárias para assinar solicitações.

Monitore seu Conta da AWS

Isso inclui Contas da AWS criar usando nossa nova AWS experiência e contas criadas usando nossa AWS experiência avançada. Para comparar as opções de inscrição, consulte [Compare as opções de inscrição](#).

O monitoramento é uma parte importante da manutenção da confiabilidade, disponibilidade e desempenho do gerenciamento de AWS contas e de suas outras AWS soluções. AWS fornece as seguintes ferramentas de monitoramento para monitorar o gerenciamento de contas, relatar quando algo está errado e tomar ações automáticas quando apropriado:

- AWS CloudTrail captura (registra) chamadas de API e eventos relacionados feitos por ou em nome de você Conta da AWS e grava os arquivos de log em um bucket do Amazon Simple Storage Service (Amazon S3) que você especificar. Isso permite que você identifique quais usuários e contas chamaram a AWS, o endereço IP de origem do qual as chamadas foram feitas e quando elas ocorreram. Para obter mais informações, consulte o [Guia do usuário do AWS CloudTrail](#).
- EventBridge A Amazon adiciona automação adicional aos seus AWS serviços respondendo automaticamente a eventos do sistema, como problemas de disponibilidade de aplicativos ou mudanças de recursos. Os eventos dos AWS serviços são entregues quase EventBridge em tempo real. Você pode escrever regras simples para determinar quais eventos são do seu interesse, e as ações automatizadas a serem tomadas quando um evento corresponder à regra. Para obter mais informações, consulte o Guia EventBridge do usuário [da Amazon](#).

Registro em log AWS Chamadas da API de gerenciamento de contas usando AWS CloudTrail

Isso inclui Contas da AWS criar usando nossa nova AWS experiência e contas criadas usando nossa AWS experiência avançada. Para comparar as opções de inscrição, consulte [Compare as opções de inscrição](#).

As APIs de gerenciamento de AWS contas são integradas AWS CloudTrail a um serviço que fornece um registro das ações realizadas por um usuário, função ou AWS serviço que chama uma operação de gerenciamento de contas. CloudTrail captura todas as chamadas da API de gerenciamento de contas como eventos. As chamadas capturadas incluem todas as chamadas para as operações do Gerenciamento de Contas. Se você criar uma trilha, poderá ativar a entrega contínua de CloudTrail eventos para um bucket do Amazon S3, incluindo eventos para operações de gerenciamento de

contas. 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 chamou uma operação de gerenciamento de contas, o endereço IP usado para fazer a solicitação, quem fez a solicitação e quando, além de detalhes adicionais.

Para saber mais CloudTrail, consulte o Guia [AWS CloudTrail do usuário](#).

Informações de gerenciamento de contas em CloudTrail

CloudTrail é ativado no seu Conta da AWS quando você cria a conta. Quando a atividade ocorre com uma operação de gerenciamento de contas, CloudTrail registra essa atividade em um CloudTrail evento junto com outros eventos AWS de serviço no histórico de eventos. Você pode visualizar, pesquisar e baixar eventos recentes em seu Conta da AWS. Para obter mais informações, consulte [Visualizar eventos com histórico de CloudTrail eventos](#).

Para um registro contínuo dos eventos em sua empresa Conta da AWS, incluindo eventos para operações de gerenciamento de contas, crie uma trilha. Uma trilha permite CloudTrail entregar arquivos de log para um bucket do Amazon S3. Por padrão, quando você cria uma trilha no Console de gerenciamento da AWS, a trilha se aplica a todas as Regiões da AWS. A trilha registra eventos de todas as regiões na partição da AWS e entrega os arquivos de log no bucket do Amazon S3 que você especifica. Você pode configurar outros AWS serviços para analisar e agir mais detalhadamente com base nos dados do evento coletados nos CloudTrail registros. Para saber mais, consulte:

- [Visão geral da criação de uma trilha](#)
- [CloudTrail serviços e integrações compatíveis](#)
- [Configuração de notificações do Amazon SNS para CloudTrail](#)
- [Recebendo arquivos de CloudTrail log de várias regiões](#)
- [Recebendo arquivos de CloudTrail log de várias contas](#)

AWS CloudTrail registra todas as operações da API de gerenciamento de contas encontradas na [seção Referência da](#) API deste guia. Por exemplo, chamadas para as PutAlternateContact operações CreateAccountDeleteAlternateContact,, e geram entradas nos arquivos de CloudTrail log.

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 de usuário root ou AWS Identity and Access Management (IAM)
- Se a solicitação tiver sido feita com credenciais de segurança temporárias de uma função do IAM ou de um usuário federado
- Se a solicitação foi feita por outro AWS serviço

Para obter mais informações, consulte [Elemento userIdentity do CloudTrail](#).

Noções básicas das entradas de log do Gerenciamento de Contas

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 operação solicitada, a data e a hora da operação, os parâmetros da solicitação e assim por diante. CloudTrail os arquivos de log não são um rastreamento de pilha ordenado das chamadas de API públicas, portanto, eles não aparecem em nenhuma ordem específica.

Exemplo 1: O exemplo a seguir mostra uma entrada de CloudTrail registro de uma chamada para a `GetAlternateContact` operação para recuperar o contato OPERATIONS alternativo atual de uma conta. Os valores retornados pela operação não estão incluídos nas informações registradas.

Example Exemplo 1

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROAI234567890EXAMPLE:AccountAPITests",
    "arn": "arn:aws:sts::123456789012:assumed-role/ServiceTestRole/AccountAPITests",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROAI234567890EXAMPLE",
        "arn": "arn:aws:iam::123456789012:role/ServiceTestRole",
        "accountId": "123456789012",
        "userName": "ServiceTestRole"
      },
    },
    "webIdFederationData": {},
```

```

    "attributes": {
      "mfaAuthenticated": "false",
      "creationDate": "2021-04-30T19:25:53Z"
    }
  },
  "eventTime": "2021-04-30T19:26:15Z",
  "eventSource": "account.amazonaws.com",
  "eventName": "GetAlternateContact",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "10.24.34.250",
  "userAgent": "Mozilla/5.0",
  "requestParameters": {
    "alternateContactType": "SECURITY"
  },
  "responseElements": null,
  "requestID": "1a2b3c4d-5e6f-1234-abcd-111111111111",
  "eventID": "1a2b3c4d-5e6f-1234-abcd-222222222222",
  "readOnly": true,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "123456789012"
}

```

Exemplo 2: O exemplo a seguir mostra uma entrada de CloudTrail registro de uma chamada para a PutAlternateContact operação para adicionar um novo contato BILLING alternativo a uma conta.

```

{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "ARO1234567890EXAMPLE:AccountAPITests",
    "arn": "arn:aws:sts::123456789012:assumed-role/ServiceTestRole/AccountAPITests",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "ARO1234567890EXAMPLE",
        "arn": "arn:aws:iam::123456789012:role/ServiceTestRole",
        "accountId": "123456789012",

```

```

    "userName": "ServiceTestRole"
  },
  "webIdFederationData": {},
  "attributes": {
    "mfaAuthenticated": "false",
    "creationDate": "2021-04-30T18:33:00Z"
  }
},
"eventTime": "2021-04-30T18:33:08Z",
"eventSource": "account.amazonaws.com",
"eventName": "PutAlternateContact",
"awsRegion": "us-east-1",
"sourceIPAddress": "10.24.34.250",
"userAgent": "Mozilla/5.0",
"requestParameters": {
  "name": "*Alejandro Rosalez*",
  "emailAddress": "alrosalez@example.com",
  "title": "CFO",
  "alternateContactType": "BILLING"
},
"responseElements": null,
"requestID": "1a2b3c4d-5e6f-1234-abcd-333333333333",
"eventID": "1a2b3c4d-5e6f-1234-abcd-444444444444",
"readOnly": false,
"eventType": "AwsApiCall",
"managementEvent": true,
"eventCategory": "Management",
"recipientAccountId": "123456789012"
}

```

Exemplo 3: O exemplo a seguir mostra uma entrada de CloudTrail registro de uma chamada para a `DeleteAlternateContact` operação para excluir o contato OPERATIONS alternativo atual.

```

{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROAI234567890EXAMPLE:AccountAPITests",
    "arn": "arn:aws:sts::123456789012:assumed-role/ServiceTestRole/AccountAPITests",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {

```

```
    "sessionIssuer": {
      "type": "Role",
      "principalId": "AROA1234567890EXAMPLE",
      "arn": "arn:aws:iam::123456789012:role/ServiceTestRole",
      "accountId": "123456789012",
      "userName": "ServiceTestRole"
    },
    "webIdFederationData": {},
    "attributes": {
      "mfaAuthenticated": "false",
      "creationDate": "2021-04-30T18:33:00Z"
    }
  },
  "eventTime": "2021-04-30T18:33:16Z",
  "eventSource": "account.amazonaws.com",
  "eventName": "DeleteAlternateContact",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "10.24.34.250",
  "userAgent": "Mozilla/5.0",
  "requestParameters": {
    "alternateContactType": "OPERATIONS"
  },
  "responseElements": null,
  "requestID": "1a2b3c4d-5e6f-1234-abcd-555555555555",
  "eventID": "1a2b3c4d-5e6f-1234-abcd-666666666666",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "123456789012"
}
```

Monitorando eventos de gerenciamento de contas com EventBridge

Isso inclui Contas da AWS você criar usando nossa nova AWS experiência e contas que você cria usando nossa AWS experiência avançada. Para comparar as opções de inscrição, consulte [Compare as opções de inscrição](#).

A Amazon EventBridge, anteriormente chamada de CloudWatch Eventos, ajuda você a monitorar eventos específicos e a iniciar ações direcionadas que usam outros. Serviços da AWS Os eventos do Serviços da AWS são entregues quase EventBridge em tempo real.

Usando EventBridge, você pode criar regras que correspondam aos eventos recebidos e encaminhá-los aos destinos para processamento.

Para obter mais informações, consulte [Introdução à Amazon EventBridge](#) no Guia do EventBridge usuário da Amazon.

Eventos do Gerenciamento de Contas

Os exemplos a seguir mostram eventos do Gerenciamento de Contas. Os eventos são emitidos com base no melhor esforço.

No momento, somente eventos específicos para ativar e desativar regiões e chamadas de API CloudTrail estão disponíveis para gerenciamento de contas.

Tipos de eventos

- [Evento para habilitar e desabilitar regiões](#)

Evento para habilitar e desabilitar regiões

Quando você habilita ou desabilita uma região em uma conta, no console ou na API, uma tarefa assíncrona é iniciada. A solicitação inicial será registrada como um CloudTrail evento na conta de destino. Além disso, um EventBridge evento será enviado para a conta chamadora quando o processo de ativação ou desativação for iniciado e novamente quando o processo for concluído.

O exemplo de evento a seguir mostra como uma solicitação será enviada indicando que, em 2020-09-30, a região ap-east-1 foi ENABLED para a conta 123456789012.

```
{
  "version": "0",
  "id": "11112222-3333-4444-5555-666677778888",
  "detail-type": "Region Opt-In Status Change",
  "source": "aws.account",
  "account": "123456789012",
  "time": "2020-09-30T06:51:08Z",
  "region": "us-east-1",
  "resources": [
```

```
    "arn:aws:account::123456789012:account"
  ],
  "detail":{
    "accountId":"123456789012",
    "regionName":"ap-east-1",
    "status":"ENABLED"
  }
}
```

Existem quatro status possíveis que correspondem aos status retornados pelas APIs `GetRegionOptStatus` e `ListRegions`:

- **ENABLED**: a região foi habilitada com êxito para o `accountId` indicado
- **ENABLING**: a região está em processo de habilitação para o `accountId` indicado
- **DISABLED**: a região foi desabilitada com êxito para o `accountId` indicado
- **DISABLING**: a região está em processo de desabilitação para o `accountId` indicado

O exemplo de padrão de evento a seguir cria uma regra que captura todos os eventos da região.

```
{
  "source":[
    "aws.account"
  ],
  "detail-type":[
    "Region Opt-In Status Change"
  ]
}
```

O exemplo de padrão de evento a seguir cria uma regra que captura somente eventos **ENABLED** de uma **DISABLED** região.

```
{
  "source":[
    "aws.account"
  ],
  "detail-type":[
    "Region Opt-In Status Change"
  ],
  "detail":{
    "status":[
```

```
        "DISABLED",  
        "ENABLED"  
    ]  
}  
}
```


Cotas para AWS Gerenciamento de contas

Você Conta da AWS tem cotas padrão, anteriormente chamadas de limites, para cada serviço. AWS

As informações de cota a seguir são para projetos que você cria se usar [Inscreva-se para AWS \(novo\)](#). Para ajustar uma cota, crie um ticket de suporte. Para obter mais informações, consulte [Apoio ao projeto](#).

Recurso	Quota	Ajustável
Número de projetos que você possui no Plano Gratuito	29	Não
Número de projetos que você pode possuir no plano pago	299	Não
Número de pessoas com quem você pode compartilhar um projeto	500	Não
Número de convites para projetos que você pode aceitar	100	Não

As informações de cota a seguir são para Contas da AWS você criar se você se inscrever usando o Sign up (avançado). Salvo indicação em contrário, cada cota é específica Região da AWS.

Recurso	Quota
Número máximo de solicitações StartPrimaryEmailUpdate por conta de destino	Três por 30 segundos
Número de contatos alternativos em um Conta da AWS	Três: cada um para BILLING, SECURITY e OPERATIONS
Número de solicitações simultâneas de opções de ativação ou desativação de uma região por conta	6

Recurso	Quota
Número de solicitações simultâneas de opções de ativação ou desativação de uma região por organização	50
Taxa de solicitações <code>AcceptPrimaryEmailUpdate</code> por conta de chamador	Uma por segundo, intermitência de até uma por segundo
Taxa de solicitações <code>DeleteAlternateContact</code> por conta	Uma por segundo, intermitência de até seis por segundo
Taxa de solicitações <code>DisableRegion</code> por conta	Uma por segundo, intermitência de até uma por segundo
Taxa de solicitações <code>EnableRegion</code> por conta	Uma por segundo, intermitência de até uma por segundo
Taxa de solicitações <code>GetAccountInformation</code> por conta de chamador	Três por segundo, intermitência de até três por segundo
Taxa de solicitações <code>GetAlternateContact</code> por conta	10 por segundo, intermitência de até 15 por segundo
Taxa de solicitações <code>GetContactInformation</code> por conta	10 por segundo, intermitência de até 15 por segundo
Taxa de solicitações <code>GetGovCloudAccountInformation</code> por conta	Três por segundo, intermitência de até cinco por segundo
Taxa de solicitações <code>GetPrimaryEmail</code> por conta de chamador	Três por segundo, intermitência de até três por segundo
Taxa de solicitações <code>GetRegionOptStatus</code> por conta	Cinco por segundo, intermitência de até cinco por segundo
Taxa de solicitações <code>ListRegions</code> por conta	Cinco por segundo, intermitência de até cinco por segundo

Recurso	Quota
Taxa de solicitações PutAccountName por conta de chamador	Uma por segundo, intermitência de até uma por segundo
Taxa de solicitações PutAlternateContact por conta	Cinco por segundo, intermitência de até oito por segundo
Taxa de solicitações PutContactInformation por conta	Cinco por segundo, intermitência de até oito por segundo
Taxa de solicitações StartPrimaryEmailUpdate por conta de chamador	Uma por segundo, intermitência de até uma por segundo

Histórico do documento para o Account Management User Guide

A tabela a seguir descreve os lançamentos da documentação para gerenciamento de AWS contas.

Alteração	Descrição	Data
Novas APIs de verificação de número de telefone	Você pode usar o novo SendPhoneNumberVerification e as VerifyPhoneNumber APIs para verificar o número de telefone do contato principal . A <code>GetContactInformation</code> resposta também inclui um novo <code>VerificationStatus</code> campo.	1º de outubro de 2026
Valores atualizados da cota de encerramento de conta	Corrigiu a porcentagem da cota de encerramento da conta de 10% para 20% e a mínima de 10 para 250 no tópico de solução de problemas.	23 de junho de 2026
Novas APIs do nome da conta	Suporte para novas GetAccountInformation e APIs PutAccountName para visualizar ou modificar o nome da conta.	22 de abril de 2025
Fim do suporte para edição das perguntas de desafio de segurança	O tópico Editar suas perguntas de desafio de segurança foi removido do guia após o término do suporte.	6 de janeiro de 2025
Novas APIs de e-mail principal	Suporte para novas APIs GetPrimaryEmail ,	6 de junho de 2024

[StartPrimaryEmailUpdate](#) e [AcceptPrimaryEmailUpdate](#) para atualizar de forma centralizada o endereço de e-mail do usuário-raiz de qualquer conta de membro no AWS Organizations. Para obter mais informações, consulte [Updating the root user email address para uma conta de membro](#) no Guia do usuário do AWS Organizations .

[Reescrita do tópico de encerramento de contas](#)

Retificação completa de todo o tópico de encerramento de contas, incluindo a adição de etapas sobre como fechar contas-membro e de gerenciamento.

1.º de fevereiro de 2024

[Fim do suporte para a adição de novas perguntas de desafio de segurança](#)

Adicionado novo conteúdo observando que a opção de adicionar novas perguntas de desafio foi removida da página Contas.

5 de janeiro de 2024

[Fim do suporte para o namespace aws-portal](#)

AWS Identity and Access Management As ações (IAM) que eram usadas anteriormente para gerenciar sua conta (por exemplo, `aws-portal:ModifyAccount` e `aws-portal:ViewAccount`) chegaram ao fim do suporte padrão.

1º de janeiro de 2024

Reescrita do tópico Regiões	Retificado por completo todo o tópico Regiões, incluindo a adição de controles para expandir e recolher.	8 de outubro de 2023
Realocados tópicos do usuário-raiz para o Guia do usuário do IAM	Consolidada a discussão sobre usuários-raiz em um tópico, adicionados links de referência cruzada aos tópicos do usuário-raiz que foram movidos para o Guia do usuário do IAM.	18 de setembro de 2023
Nova seção adicionada ao tópico de contato da conta principal	Adicionada uma nova seção Requisitos de número de telefone e endereço de e-mail.	12 de setembro de 2023
Novas APIs de informações de contato	Suporte para novas APIs <code>GetContactInformation</code> e <code>PutContactInformation</code> .	22 de julho de 2022
AWS O gerenciamento de contas agora suporta a atualização de contatos alternativos por meio do AWS Organizations console.	Agora você pode atualizar os contatos alternativos da sua organização por meio do AWS Organizations console usando as permissões da API de conta fornecidas pelas políticas AWS Organizations gerenciadas atualizadas.	8 de fevereiro de 2022
Lançamento inicial	Versão inicial do Guia de referência de gerenciamento de AWS contas	30 de setembro de 2021

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.