Benutzer-Leitfaden

AWS Control Tower

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

AWS Control Tower: Benutzer-Leitfaden

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

Die Handelsmarken und die Handelsaufmachung von Amazon dürfen nicht in einer Weise in Verbindung mit nicht von Amazon stammenden Produkten oder Services verwendet werden, durch die Kunden irregeführt werden könnten oder Amazon in schlechtem Licht dargestellt oder diskreditiert werden könnte. Alle anderen Handelsmarken, die nicht Eigentum von Amazon sind, gehören den jeweiligen Besitzern, die möglicherweise zu Amazon gehören oder nicht, mit Amazon verbunden sind oder von Amazon gesponsert werden.

Table of Contents

Was ist der AWS Control Tower? 1
Features 1
Wie der AWS Control Tower mit anderen interagiert AWS service 2
Sind Sie ein First-Time Benutzer von AWS Control Tower? 3
Funktionsweise 4
Struktur einer AWS-Kontrollturm-Landezone 4
Was passiert, wenn Sie eine landing zone einrichten 5
Was sind die gemeinsamen Konten? 6
Wie funktionieren Steuerungen 7
So funktioniert AWS Control Tower mit StackSets 8
Terminologie 9
Preisgestaltung 13
Einrichtung 14
Melden Sie sich an für AWS 14
Melde dich an für ein AWS-Konto 14
Nächster Schritt 14
Erste Schritte 15
Schnellstart-Anleitung 15
Pre-launch Schecks 17
Überlegungen für AWS IAM Identity Center (IAM Identity Center) -Kunden 18
Richten Sie eine spezielle Umgebung für Ihre Steuerungen ein 19
Erste Schritte 20
Überlegungen zur AWS-Konfiguration 20
Implementierungsprozess 20
Wichtige Hinweise 21
Beginnen Sie von der Konsole aus 21
Erwartungen an die Konfiguration der Landezone 21
Schritt 1: Erstellen Sie die E-Mail-Adressen für Ihr gemeinsames Konto 23
Schritt 2. Konfiguriere und starte deine Landezone 24
Schritt 3. Überprüfe die Landezone und richte sie ein 34
Erste Schritte mit der Verwendung von APIs 35
Erwartungen an die Konfiguration der landing zone mit APIs 36
Schritt 1: Konfiguriere deine landing zone 37
Schritt 2: Starten Sie Ihre landing zone mithilfe der AWS Control Tower Tower-APIs 41

Identifizieren Sie Ihre landing zone 44
Aktualisiere deine landing zone 45
Setze die landing zone zurück, um Drift zu beheben 47
Sehen Sie sich die Details Ihrer Landezonen-Manifestdatei an 48
Sehen Sie sich den Status Ihrer Landezonenoperationen an 53
Beispiele: Richten Sie eine AWS Control Tower-Landezone nur mit APIs ein 55
Landezonenschemata 63
Starte eine landing zone mit CloudFormation 86
Nächste Schritte 92
Einschränkungen und Kontingente 93
Bekannte Einschränkungen in AWS Control Tower 93
Anfordern einer Kontingenterhöhung 96
Einschränkungen bei der Steuerung 98
Finden Sie verfügbare Steuerelemente und Regionen 99
Einschränkungen, die auf dem zugrunde liegenden Grund basieren AWS service 99
Regionale Unterschiede 101
Das Referenzhandbuch für Steuerelemente 103
Bewährte Methoden für Administratoren 104
Erläuterung des Zugriffs für Benutzer 104
Erläuterung des Ressourcenzugriffs 104
Erläuterung präventiver Kontrollen 105
Plane deine landing zone 106
Funktionen vergleichen 107
Starten Sie AWS Control Tower in einer bestehenden Organisation 108
Starten Sie AWS Control Tower in einer neuen Organisation 110
Bewährte Methoden: Richten Sie eine landing zone für AWS mehrere Konten ein 110
Halten Sie sich an die Leitlinien für AWS mehrere Konten 111
Richtlinien für die Einrichtung einer gut strukturierten Umgebung 112
Passen Sie Ihre OU-Struktur an AWS Strategie für mehrere Konten 115
Über den Root 115
Administrative Tipps für die Einrichtung der landing zone 116
Leitfaden zur Migration von Landing Zone v4.0 117
Die wichtigsten Änderungen 118
Aktualisierungen der AWS Config 121
Vergleich der Funktionen mit und ohne AWS Config Integration 125
Empfehlungen für die Einrichtung von Gruppen, Rollen und Richtlinien 127

Hinweise zu AWS Control Tower Tower-Ressourcen ... 128
Wann sollten Sie sich als Root-Benutzer anmelden ... 130
AWS Organizations Anleitungen ... 131
Anleitung zum IAM Identity Center ... 133
Anleitung von Account Factory ... 135
Hinweise zum Abonnieren von SNS-Themen ... 136
Anleitung für KMS-Schlüssel ... 137
Aktualisierungen der Landezone ... 138
Richtlinien für AI-based Dienste ... 141
Verwaltung von Konfigurationsupdates ... 142
Über Updates ... 144
Aktualisiere deine landing zone ... 145
Standardverfahren für Updates ... 145
Wählen Sie eine Landezonenversion ... 146
Kontoaktualisierungen, Landingzone-Versionen und Baselines ... 147
Kontospuren beibehalten ... 148
Beheben Sie Abweichungen mit Reset und Re-register ... 150
Konten mithilfe von Automatisierung bereitstellen und aktualisieren ... 151
Automatisieren Sie Aufgaben ... 153
AWS CloudShell und der AWS CLI ... 156
Besorgen Sie sich IAM-Berechtigungen für AWS CloudShell ... 156
Interagiere mit AWS Control Tower durch AWS CloudShell ... 157
AWS CloudFormation Ressourcen ... 160
AWS Control Tower und CloudFormation Vorlagen ... 161
Erfahren Sie mehr über CloudFormation ... 161
Passen Sie Ihre Landezone an ... 162
Passen Sie es von der AWS Control Tower-Konsole aus an ... 162
Automatisieren Sie Anpassungen außerhalb der AWS Control Tower-Konsole ... 164
AWS Control Tower und LZA ... 164
Vorteile von Anpassungen für AWS Control Tower (cFCT) ... 165
Weitere cFCT-Beispiele ... 166
Übersicht über Anpassungen für AWS Control Tower (cFCT) ... 167
Architektur ... 168
Cost (Kosten) ... 170
Komponentendienste ... 171
AWS CodeCommit ... 171

AWS CodePipeline ... 171
AWS Key Management Service ... 172
AWS Lambda ... 172
Amazon Simple Notification Service ... 172
Amazon Simple Storage Service ... 172
Amazon Simple Queue Service ... 173
AWS Step Functions ... 173
AWS Systems Manager Parameter Store ... 173
Überlegungen zur Bereitstellung ... 173
Bereiten Sie sich auf die Bereitstellung vor ... 174
Um Anpassungen für AWS Control Tower zu aktualisieren ... 175
Vorlage und Quellcode ... 175
Quellcode ... 176
CFCT bereitstellen ... 176
Voraussetzungen ... 176
Schritte zur Bereitstellung ... 176
Schritt 1. Starten des -Stacks ... 177
Schritt 2. Erstellen Sie ein benutzerdefiniertes Paket ... 181
Aktualisieren Sie den Stack ... 181
Löschen eines Stack-Sets ... 182
Amazon S3 als Konfigurationsquelle einrichten ... 184
GitHub Als Konfigurationsquelle einrichten ... 185
Bereite ein GitHub Repository vor ... 185
Erstellen Sie die Verbindung GitHub ... 185
Stellen Sie das bereit CloudFormation Stack ... 186
Operationelle Metriken ... 186
Leitfaden zur cFCT-Anpassung ... 187
Überblick über die Code-Pipeline ... 188
Definieren Sie eine benutzerdefinierte Konfiguration ... 190
Root-OU ... 197
Verschachtelte Organisationseinheit ... 199
Erstellen Sie Ihre eigenen Anpassungen ... 200
Versions-Upgrades für das cFCT-Manifest ... 208
Netzwerk ... 211
VPCs und AWS Regionen im AWS Control Tower ... 211
Überblick über AWS Control Tower und VPCs ... 212

CIDR und Peering für VPC und AWS Control Tower ... 214
AWS PrivateLink ... 215
Überlegungen ... 216
Erstellen eines Schnittstellenendpunkts ... 216
Erstellen einer Endpunktrichtlinie ... 216
Rollen und Berechtigungen ... 218
Rollen und Konten ... 219
Rollen und Kontoerstellung ... 219
AWSControlTowerExecution Rolle ... 220
Optionale Bedingungen für Ihre Rolle, Ihre Vertrauensbeziehungen ... 221
So aggregiert AWS Control Tower AWS Config Regeln in nicht verwalteten Organisationseinheiten und Konten ... 224
Programmgesteuerte Rollen und Vertrauensbeziehungen für das AWS Control Tower Tower-Auditkonto ... 227
Automatisierte Kontobereitstellung mit IAM-Rollen ... 231
Ressourcen verwalten ... 233
Regionen konfigurieren ... 234
Konfigurieren Sie Ihre AWS Control Tower-Regionen ... 235
Vermeiden Sie eine gemischte Steuerung bei der Konfiguration von Regionen ... 238
Über Opt-in-Regionen ... 239
Konfigurieren Sie die Region Deny Control ... 242
Überlegungen zur OU-level Region verweigern die Kontrolle ... 244
Informationen zu -Konten ... 245
Was passiert, wenn AWS Control Tower ein Konto erstellt ... 245
Überlegungen zur Verwendung vorhandener Sicherheits- oder Protokollkonten ... 246
Konten zur Serviceintegration ... 247
Verwaltungskonto ... 247
CloudTrail Administratorkonto ... 248
Aggregatorkonto konfigurieren ... 249
Ressourcen für das Serviceintegrationskonto ... 250
Ressourcen für Verwaltungskonten ... 250
CloudTrail Ressourcen für Administratorkonten ... 255
Ressourcen für Config-Aggregatorkonten ... 258
Über Mitgliedskonten ... 261
Interagieren Sie mit AWS Control Tower Tower-Konten von AWS Service Catalog ... 262
Erstellen Sie ein Konto und stellen Sie es bereit ... 262

Automatisieren Sie die Kontobereitstellung in AWS Control Tower mithilfe von Service Catalog-APIs ... 264
Aktualisieren Sie das bereitgestellte Produkt im Service Catalog ... 268
Ein Konto im Service Catalog deregistrieren ... 270
Bereitstellung und Verwaltung von Konten ... 272
Erforderliche Berechtigungen ... 272
Methoden der Bereitstellung ... 273
Konten in der Konsole bereitstellen ... 275
Sehen Sie sich Ihre Konten an ... 276
Über das Registrieren von Konten ... 277
Was passiert bei der Kontoregistrierung ... 278
Registrieren Sie bestehende Konten bei VPCs ... 279
Registrieren Sie Konten bei AWS Config Ressourcen ... 280
Voraussetzungen für die Immatrikulation ... 280
Auto-enrollment Option ... 283
Melden Sie sich von der Konsole aus an ... 285
Wenn das Konto die Voraussetzungen nicht erfüllt ... 289
Fügen Sie die erforderliche IAM-Rolle manuell zu einer vorhandenen hinzu AWS-Konto und registriere es ... 291
Konten registrieren, die bereits vorhanden sind AWS Config Ressourcen ... 294
Schritt 1: Wenden Sie sich an den Support, um Konten zur Zulassungsliste hinzuzufügen ... 296
Schritt 2: Erstellen Sie eine neue IAM-Rolle im Mitgliedskonto ... 297
Schritt 3: Identifizieren Sie AWS Regionen mit bereits vorhandenen Ressourcen ... 298
Schritt 4: Identifizieren Sie AWS Regionen ohne AWS Config Ressourcen ... 298
Schritt 5: Ändern Sie die vorhandenen Ressourcen in jeder AWS Region ... 298
Schritt 5a. AWS Config Ressourcen für Rekorder ... 299
Schritt 5b. Modifizieren Sie AWS Config Ressourcen für den Lieferkanal ... 300
Schritt 5c. Modifizieren Sie AWS Config Ressourcen für die Aggregation und Autorisierung ... 300
Schritt 6: Ressourcen dort erstellen, wo sie nicht existieren, in Regionen, die von AWS Control Tower verwaltet werden ... 301
Schritt 7: Registrieren Sie die Organisationseinheit bei AWS Control Tower ... 303
Account Factory ... 303
Berechtigungen ... 303
Überlegungen zum Konto ... 304
Konten aktualisieren und verschieben ... 305

E-Mail-Adresse eines registrierten Kontos ändern ... 306
Ändern Sie den Namen eines registrierten Kontos ... 307
Konfigurieren Sie die Amazon VPC-Einstellungen ... 308
Ein Konto abmelden ... 310
Ein Konto schließen ... 311
Ressourcen von Account Factory ... 313
Account Factory-Anpassung (AFC) ... 315
Für die Anpassung einrichten ... 318
Erstellen Sie ein benutzerdefiniertes Konto anhand eines Blueprints ... 325
Passen Sie Konten bei AFC an, während Sie sie registrieren ... 326
Fügen Sie einem AWS Control Tower-Konto einen Blueprint hinzu ... 326
Aktualisieren Sie einen Blueprint ... 327
Einen Blueprint aus einem Konto entfernen ... 328
Pläne von Partnern ... 328
Überlegungen zu Account Factory-Anpassungen (AFC) ... 329
Im Falle eines Blueprint-Fehlers ... 329
Anpassung Ihres Richtliniendokuments für AFC-Blueprints auf der Grundlage von CloudFormation ... 331
Für die Erstellung eines Terraform-based Service Catalog-Produkts sind zusätzliche Berechtigungen erforderlich ... 333
Übergang zum externen Produkttyp ... 334
AWS Control Tower Account Factory für Terraform (AFT) ... 335
Voraussetzungen ... 336
AFT im Überblick ... 337
Stellen Sie AFT bereit ... 340
Stellen Sie ein neues Konto bereit ... 350
Mehrere Kontoanfragen ... 352
Aktualisieren Sie ein vorhandenes Konto ... 352
Unterstützte Versionen ... 355
Funktionsoptionen aktivieren ... 359
Ressourcen für AFT ... 364
Erforderliche Rollen ... 369
Komponentendienste ... 372
Pipeline für die Bereitstellung von AFT-Konten ... 374
Anpassungen des Kontos ... 377
Auslöser für die Anpassung ... 386

Alternatives VCS ... 389
Datenschutz ... 393
Ein Konto entfernen ... 394
Operationelle Metriken ... 396
Anleitung zur Fehlerbehebung ... 397
Abweichungen ... 401
Drift erkennen ... 401
Meinungsverschiedenheiten ... 403
Behebung von Abweichungen ... 404
Überlegungen zu Drift- und Policy-Scans ... 405
Arten von Abweichungen, die sofort behoben werden müssen ... 406
Reparierbare Änderungen an Ressourcen ... 407
Drift und Bereitstellung neuer Konten ... 408
Arten von Abweichungen in der Unternehmensführung ... 408
Mitgliedskonto wurde verschoben ... 411
Mitgliedskonto wurde entfernt ... 413
Ungeplantes Update auf Managed SCP ... 414
SCP wurde von der verwalteten Organisationseinheit getrennt ... 415
Die grundlegende Organisationseinheit wurde gelöscht ... 416
Security Hub CSPM — Drift bei der Steuerung ... 417
Kontrollieren Sie die Abweichung der Richtlinien ... 418
Vertrauenswürdiger Zugriff deaktiviert ... 419
Vererbungsabweichung bei aktivierten Baselines ... 420
Vererbungsabweichung bei aktivierten Steuerelementen ... 421
EventBridge Schöpfung ... 423
Wenn Sie Ressourcen außerhalb von AWS Control Tower verwalten ... 425
Bezieht sich auf Ressourcen außerhalb von AWS Control Tower ... 426
Externe Änderung der AWS-Control-Tower-Ressourcennamen ... 427
Löschen der Sicherheits-Organisationseinheit ... 427
Ein Konto aus der Sicherheits-OU entfernen ... 428
Externe Änderungen, die automatisch aktualisiert werden ... 431
Organizations ... 434
Video-Anleitung ... 435
Topics ... 435
Erweitern Sie die Unternehmensführung auf eine bestehende Organisation ... 435
Video: Aktiviere eine Landing Zone in einer bestehenden AWS Organizations ... 437

Überlegungen für IAM Identity Center und bestehende Organisationen ... 437
Zugriff auf andere AWS service ... 438
Verschachtelte OUs ... 438
Video-Anleitung ... 438
Erweitern Sie von der flachen OU-Struktur zur verschachtelten OU-Struktur ... 438
Die Registrierung verschachtelter OU wird vorab überprüft ... 439
Verschachtelte Organisationseinheiten und Rollen ... 440
Was passiert bei der Registrierung und erneuten Registrierung von verschachtelten Organisationseinheiten und Konten ... 440
Überlegungen zur Registrierung verschachtelter Organisationseinheiten ... 441
Einschränkungen bei verschachtelten Organisationseinheiten ... 441
Verschachtelte Organisationseinheiten und Compliance ... 441
Verschachtelte Organisationseinheiten und Drift ... 442
Verschachtelte Organisationseinheiten und Kontrollen ... 443
Verschachtelte Organisationseinheiten und der Stamm ... 444
Registrieren Sie eine OU, um mehrere Konten zu registrieren ... 445
Eine bestehende OU registrieren ... 446
Erstellen Sie eine neue OU ... 448
Eine Organisationseinheit entfernen ... 449
Häufige Fehlerursachen bei der Registrierung oder erneuten Registrierung ... 451
Organisationen aktualisieren ... 454
Wann müssen OUs und Konten aktualisiert werden ... 454
Aktualisieren Sie mehrere Konten in einer Organisationseinheit ... 454
Was passiert bei der erneuten Registrierung ... 455
Aktualisieren Sie ein einzelnes Konto ... 456
Ein Konto übertragen ... 457
Voraussetzungen ... 457
Schritt 1: Das Konto bei AWS Control Tower abmelden ... 457
Schritt 2: Übertragen Sie das Konto an die Zielorganisation ... 458
Schritt 3: Registrieren Sie das Konto bei der Zielorganisation ... 458
Weitere Überlegungen ... 458
Integrierte Services ... 460
AWS Datensicherung ... 460
CloudFormation ... 461
CloudTrail ... 461
CloudWatch ... 461

AWS Config ... 462
Integration von AWS Config in die Control Tower Landing Zone 4.0 ... 462
AWS Identity and Access Management ... 465
AWS Key Management Service ... 466
AWS Lambda ... 466
AWS Organizations ... 466
Überlegungen ... 467
Amazon S3 ... 467
Security Hub CSPM ... 468
AWS Service Catalog ... 468
Amazon SNS ... 468
Step-Funktionen ... 469
Identity and Access Management ... 470
Authentifizierung ... 470
Zugriffskontrolle ... 473
IAM Identity Center und AWS Control Tower ... 473
Benutzergruppen, Rollen und Berechtigungssätze ... 474
Wissenswertes über IAM Identity Center-Konten und AWS Control Tower ... 475
IAM Identity Center-Gruppen für AWS Control Tower ... 476
Überblick über die Verwaltung des Ressourcenzugriffs mit IAM ... 479
Ressourcen und Betrieb des AWS Control Tower ... 480
Über den Besitz von Ressourcen ... 481
Verwalte den Zugriff auf Ressourcen ... 481
Geben Sie die Richtlinienelemente an: Aktionen, Auswirkungen und Prinzipien ... 493
Angeben von Bedingungen in einer Richtlinie ... 494
Beugen Sie verwirrten Angriffen durch Abgeordnete vor ... 494
IAM-Richtlinien für AWS Control Tower ... 495
Für die Verwendung der AWS Control Tower-Konsole sind Berechtigungen erforderlich ... 495
AWS ControlTowerAdmin Rolle ... 497
AWS ControlTowerServiceRolePolicy ... 498
AWS ControlTowerIdentityCenterManagementPolicy ... 499
AWS ControlTowerStackSetRole ... 500
AWS ControlTowerCloudTrailRolePolicy ... 501
AWS ControlTowerBlueprintAccess Anforderungen an die Rolle ... 502
AWSServiceRoleForAWSControlTower ... 504
AWS ControlTowerAccountServiceRolePolicy ... 504

Verwaltete Richtlinien für AWS Control Tower 505
Sicherheit 517
Datenschutz 517
Verschlüsselung im Ruhezustand 519
Verschlüsselung während der Übertragung 519
Einschränken des Zugriffs auf Inhalte 519
Compliance-Validierung 520
Ausfallsicherheit 521
Infrastruktursicherheit 521
Protokollieren und Überwachen 523
Über die Anmeldung bei AWS Control Tower 524
S3-Bucket-Richtlinie 525
Landing Zone Version 3.3 und früher 525
Landing Zone Version 4.0 und höher 527
Überblick über die Überwachung 530
Protokollierung von AWS Control Tower-Aktionen mit AWS CloudTrail 531
Informationen zum AWS Control Tower finden Sie unter CloudTrail 531
Beispiel: Einträge in der AWS Control Tower-Protokolldatei 534
Überwachen Sie Ressourcenänderungen mit AWS Config 535
Config-Kosten verwalten 536
Sehen Sie sich die an AWS Config Rekorderdaten zu registrierten Konten 538
Fehlerbehebung AWS Config im AWS Control Tower 539
Ereignisse im Lebenszyklus 540
`CreateManagedAccount` 544
`UpdateManagedAccount` 546
`EnableGuardrail` 547
`DisableGuardrail` 548
`SetupLandingZone` 550
`UpdateLandingZone` 552
`RegisterOrganizationalUnit` 554
`DeregisterOrganizationalUnit` 555
`PrecheckOrganizationalUnit` 556
`EnableBaseline` 558
`ResetEnabledBaseline` 560
`UpdateEnabledBaseline` 561
`DisableBaseline` 562

EnableControl ... 564
ResetEnabledControl ... 566
UpdateEnabledControl ... 567
DisableControl ... 568
Benutzerbenachrichtigungen ... 570
Backup ... 573
Voraussetzungen ... 574
Backups aktivieren ... 576
Erster Teil: Richten Sie Backups für Ihre landing zone ein ... 576
Nächster Teil: Backups auf Organisationseinheiten aktivieren ... 578
Schalten Sie Backups aus ... 580
Erster Schritt: Schalten Sie Backups auf Organisationseinheiten aus ... 580
Nächster Schritt: Ausschalten AWS Backup für deine landing zone ... 582
Konten wurden verschoben ... 582
Backup-Drift ... 583
Ressourcen Backup ... 584
Kontrollen für AWS Backup ... 588
Eine landing zone stilllegen ... 589
Überblick über den Außerbetriebnahmeprozess ... 590
Wie man eine landing zone außer Betrieb nimmt ... 591
Machen Sie Ihre landing zone mit APIs außer Betrieb ... 593
Nach der Außerbetriebnahme sind manuelle Aufräumarbeiten erforderlich ... 593
Ressourcen, die bei der Außerbetriebnahme nicht entfernt wurden ... 595
AWS Control Tower Tower-Ressourcen entfernen ... 598
Muss ich außer Betrieb nehmen, anstatt zu löschen? ... 599
Über das Entfernen von AWS Control Tower Tower-Ressourcen ... 600
Löschen SCPs ... 600
Löschen und Stapel StackSets ... 601
Löschen Sie Amazon S3 S3-Buckets im Log Archive-Konto ... 602
Ein Konto entfernen, ein Factory-Portfolio und ein Produkt ... 603
Rollen und Richtlinien von AWS Control Tower entfernen ... 604
Hilfe zu den Ressourcen von AWS Control Tower ... 606
Einrichtung nach der Außerbetriebnahme einer landing zone ... 606
Anleitungen ... 608
Exemplarische Vorgehensweise: Wechseln Sie von ALZ zum AWS Control Tower ... 608
Exemplarische Vorgehensweise: Konfiguration des AWS Control Tower ohne VPC ... 609

Löschen Sie die AWS Control Tower VPC ... 609
Bereinigen Sie optional die VPC-Ressource im Konto ... 610
Erstellen Sie ein Konto in AWS Control Tower ohne VPC ... 610
Exemplarische Vorgehensweise: Einrichten von Sicherheitsgruppen im AWS Control Tower mit AWS Firewall Manager ... 612
Richten Sie Sicherheitsgruppen ein mit AWS Firewall Manager ... 612
Fehlerbehebung ... 613
Start der Landing Zone fehlgeschlagen ... 613
Die Aktualisierung der Landing Zone ist mit einem KMS-Fehler fehlgeschlagen ... 614
Die Landing Zone konnte nicht aktualisiert werden ... 615
Fehler „Landezone ist nicht aktuell“ ... 616
New Account Provisioning Failed (Bereitstellung eines neuen Kontos fehlgeschlagen) ... 617
Ein bestehendes Konto konnte nicht angemeldet werden ... 618
Ein Account Factory-Konto konnte nicht aktualisiert werden ... 619
Fehler: Erwähnter Fehler AWS Config ... 620
Portfoliofehler bei AWS Control Tower Account Factory ... 622
Fehler „Unzureichende Berechtigungen“ erhalten ... 623
Detektivkontrollen wirken sich nicht auf Konten aus ... 623
Der Fehler „Rate überschritten“ wurde zurückgegeben von AWS Organizations API ... 624
Fehler beim Verschieben eines Account Factory Factory-Kontos direkt von einer AWS Control Tower Tower-Landezone in eine andere AWS Control Tower Tower-Landezone ... 625
AWS Support ... 627
Baselines ... 628
Basistypen, die auf OU-Ebene gelten ... 628
Basistypen, die bei der Einrichtung der landing zone für Serviceintegrationskonten gelten ... 630
Teilweise Registrierung ... 632
Vergleichen Sie Konsole und API ... 632
Aktivierte Baselines und Mitgliedskonten ... 633
Baselines und Standardeinstellungen für die Versionierung ... 634
AWSControlTowerBaseline Tabelle ... 634
Beispiele: Registrieren Sie eine AWS Control Tower-OU nur mit APIs ... 640
Basis-API-Beispiele ... 643
`DisableBaseline` ... 643
`EnableBaseline` ... 643
`GetBaseline` ... 645
`GetBaselineOperation` ... 646

GetEnabledBaseline ... 647
ListBaselines ... 648
ListEnabledBaselines ... 649
ResetEnabledBaseline ... 654
UpdateEnabledBaseline ... 655
Zusätzliche Informationen ... 657
Tutorials und Übungen ... 657
Netzwerk ... 211
Sicherheit, Identität und Protokollierung ... 658
Bereitstellung von Ressourcen und Verwaltung von Workloads ... 659
Zusammenarbeit mit bestehenden Organisationen und Konten ... 659
Automatisierung und Integration ... 659
Migration von Workloads ... 660
Zugehörige AWS-Services ... 660
AWS Marketplace Lösungen ... 661
Versionshinweise ... 662
Januar 2026 - Heute ... 662
Account Factory for Terraform (AFT) unterstützt reine Plananpassungsläufe ... 662
AWS Control Tower ist in der europäischen Sovereign Cloud verfügbar ... 663
Januar 2025 — Dezember 2025 ... 663
Version 4.0 der AWS Control Tower-Landezone ... 664
AWS Control Tower fügt weitere 279 hinzu AWS Config Steuerungen für Control Catalog ... 666
AWS Control Tower ist in der Region Asien-Pazifik (Neuseeland) verfügbar ... 666
AWS Control Tower unterstützt die automatische Kontoregistrierung ... 666
AWS Control Tower aktualisiert die Python-Version ... 667
Der AWS Control Tower reduziert die Drift ... 667
AWS Control Tower unterstützt IPv6-Adressen ... 668
Account Factory für Terraform Version 1.15.0 verfügbar ... 668
Die Steuerelemente mit Nitro-Instanztypen wurden aktualisiert ... 668
AWS Control Tower ist in der Region Asien-Pazifik (Taipeh) verfügbar ... 670
AWS Control Tower unterstützt PrivateLink ... 670
Unterstützung für zusätzliche Branchen-Frameworks, aktualisierte Metadaten ... 670
Service-linked AWS Config Steuerelemente ... 671
Die Konsolenansicht mit aktivierten Steuerelementen bietet eine zentrale Übersicht ... 673
Account Factory for Terraform (AFT) unterstützt neue Konfigurationen bei der Bereitstellung ... 674

AWS Control Tower führt Berichte auf Kontoebene für Basis-APIs ein 674
AWS Control Tower ist verfügbar in AWS Regionen Asien-Pazifik (Thailand) und Mexiko (Zentral) 675
Zusätzliche AWS Config Steuerungen verfügbar 675
Heben Sie die Registrierung von Aktionen für Organisationseinheiten auf und löschen Sie sie 676
Control Catalog unterstützt IPv6-Adressen 676
Januar — Dezember 2024 676
AWS Control Tower CFCT unterstützt GitHub und RCPs 677
AWS Control Tower fügt präventive Kontrollen mit deklarativen Richtlinien hinzu 678
AWS Control Tower bietet Optionen für präskriptive Backup-Pläne 678
AWS Control Tower ist integriert AWS Config Steuerelemente 678
AWS Control Tower verbessert das Hook-Management und fügt proaktive Kontrollregionen hinzu 679
AWS Control Tower führt Richtlinien für die Verwaltung von Ressourcen ein 680
AWS Control Tower meldet eine Abweichung der Kontrollrichtlinien 680
Neue `ResetEnabledControl` API 681
`GetControl`API zur Steuerung von Katalogaktualisierungen 681
AWS Control Tower AFT unterstützt GitLab 682
AWS Control Tower ist verfügbar in AWS Asien-Pazifik (Malaysia) 682
AWS Control Tower unterstützt bis zu 1000 Konten pro OU 682
AWS Control Tower fügt eine Versionsauswahl für die Landezone hinzu 683
Beschreibende Kontroll-API verfügbar, erweiterter Zugriff auf Regionen und Steuerelemente 683
AWS Control Tower unterstützt AFT und cFCT in Opt-in-Regionen 684
AWS Control Tower fügt die `ListLandingZoneOperations` API hinzu 685
AWS Control Tower unterstützt bis zu 100 gleichzeitige Kontrollvorgänge 685
AWS Control Tower ist verfügbar in AWS Kanada West (Calgary) 686
AWS Control Tower unterstützt Self-Service-Kontingentanpassungen 687
AWS Control Tower veröffentlicht den Referenzhandbuch für Steuerungen 688
AWS Control Tower aktualisiert zwei proaktive Kontrollen und benennt sie um 688
Veraltete Steuerelemente sind nicht mehr verfügbar 689
AWS Control Tower unterstützt das Taggen von `EnabledControl` Ressourcen in CloudFormation 689
AWS Control Tower unterstützt APIs für die Registrierung und Konfiguration von Organisationseinheiten mit Baselines 690

Januar — Dezember 2023 691
Übergang zu neuen AWS Service Catalog Externer Produkttyp (Phase 3) 692
AWS Control Tower-Landingzone, Version 3.3 693
Übergang zu neuen AWS Service Catalog Externer Produkttyp (Phase 2) 694
Der AWS Control Tower kündigt Kontrollen zur Unterstützung der digitalen Souveränität an 694
APIs für die Landezone von AWS Control Tower 698
APIs für das Taggen von AWS Control Tower Control 698
AWS Control Tower ist verfügbar in AWS Asien-Pazifik (Melbourne) 699
Übergang zu neuen AWS Service Catalog Externer Produkttyp (Phase 1) 699
AWS Control Tower fügt eine neue Kontroll-API hinzu 699
AWS Control Tower fügt neue Steuerungen hinzu 700
AWS Control Tower erkennt vertrauenswürdige Zugriffsabweichungen 700
AWS Control Tower ist in vier weiteren Versionen erhältlich AWS-Regionen 700
AWS Control Tower verfügbar in AWS Israel (Tel Aviv) 701
AWS Control Tower fügt 28 neue proaktive Kontrollen hinzu 701
Im AWS Control Tower sind zwei Steuerelemente veraltet 701
AWS-Kontrollturm-Landezone, Version 3.2 702
AWS Control Tower fügt die Zuordnung von E-Mail zu ID für IAM Identity Center hinzu 703
AWS Control Tower fügt weitere hinzu AWS Security Hub CSPM Steuerelemente 704
AWS Control Tower veröffentlicht Metadaten für AWS Security Hub CSPM Steuerelemente 704
AWS Control Tower fügt Account Factory Customization (AFC) für Terraform hinzu 705
AWS Control Tower fügt ein selbstverwaltetes IAM-Identitätscenter hinzu 705
AWS Control Tower fügt einen gemischten Hinweis zur Unternehmensführung hinzu 705
AWS Control Tower fügt neue proaktive Kontrollen hinzu 706
AWS Control Tower aktualisiert die Amazon EC2-Steuerelemente 706
AWS Control Tower ist in sieben weiteren erhältlich AWS-Regionen 706
AWS Control Tower Account Factory Customization (AFC) und Anforderungsverfolgung sind allgemein verfügbar 707
AWS Control Tower-Landezone, Version 3.1 707
Proaktive Kontrollen im AWS Control Tower sind allgemein verfügbar 709
Januar — Dezember 2022 709
Gleichzeitige Kontooperationen 710
Factory-Anpassung des Kontos (AFC) 710
Umfassende Kontrollen helfen bei AWS Bereitstellung und Verwaltung von Ressourcen 711

Der Konformitätsstatus ist für alle sichtbar AWS Config Regeln 712
API für Kontrollen und eine neue CloudFormation Ressource 712
cFCT unterstützt das Löschen von Stack-Sets 713
Benutzerdefinierte Aufbewahrung von Protokollen 714
Role-Drift-Reparatur verfügbar 714
AWS Control Tower-Landezone, Version 3.0 714
Die Seite Organisation kombiniert Ansichten von Organisationseinheiten und Konten 718
Vereinfachte Kontoerstellung und Registrierung 719
AFT unterstützt die automatische Anpassung für gemeinsam genutzte AWS Control Tower-Konten 719
Gleichzeitige Operationen für alle optionalen Steuerungen 720
Bestehende Sicherheits- und Logging-Konten 721
AWS Control Tower-Landingzone, Version 2.9 722
AWS-Kontrollturm-Landezone, Version 2.8 722
Januar — Dezember 2021 723
Funktionen zur Sperrung von Regionen 724
Funktionen zur Datenresidenz 724
AWS Control Tower führt die Bereitstellung und Anpassung von Terraform-Konten ein 725
Neues Lifecycle-Ereignis verfügbar 726
AWS Control Tower ermöglicht verschachtelte OUs 726
Parallelität bei der Detektivkontrolle 727
Zwei neue Regionen verfügbar 728
Abwahl der Region 728
AWS Control Tower funktioniert mit AWS Wichtige Managementsysteme 729
Steuerung umbenannt, Funktionalität unverändert 730
Der AWS Control Tower scannt täglich SCPs, um nach Abweichungen zu suchen 730
Benutzerdefinierte Namen für Organisationseinheiten und Konten 730
AWS Control Tower-Landezone, Version 2.7 731
Drei neue AWS Regionen verfügbar 733
Nur ausgewählte Regionen verwalten 733
AWS Control Tower dehnt die Governance jetzt auf bestehende Organisationseinheiten in Ihrem Unternehmen aus AWS Organisationen 734
AWS Control Tower bietet massenweise Kontoaktualisierungen 734
Januar — Dezember 2020 735
Die AWS Control Tower-Konsole ist jetzt mit externen Geräten verknüpft AWS Konfigurationsregeln 735

AWS Control Tower ist jetzt in weiteren Regionen verfügbar 736
Aktualisierung der Leitplanke 737
Die AWS Control Tower-Konsole zeigt mehr Details zu OUs und Konten 737
Verwenden Sie AWS Control Tower, um ein neues Multikonto einzurichten AWS Umgebungen in AWS Organizations 737
Anpassungen für die AWS Control Tower-Lösung 738
Allgemeine Verfügbarkeit von AWS Control Tower Version 2.3 739
Single-step Bereitstellung von Konten im AWS Control Tower 739
Tool zur Außerbetriebnahme von AWS Control Tower 740
Benachrichtigungen über Ereignisse im Lebenszyklus von AWS Control Tower 741
Juni — Dezember 2019 741
Allgemeine Verfügbarkeit von AWS Control Tower Version 2.2 742
Neue optionale Steuerungen im AWS Control Tower 742
Neue Detektivkontrollen im AWS Control Tower 743
AWS Control Tower akzeptiert E-Mail-Adressen für gemeinsam genutzte Konten mit anderen Domänen als das Verwaltungskonto 743
Allgemeine Verfügbarkeit von AWS Control Tower Version 2.1 744
Dokumentverlauf 745
AWS Glossar 772
..... dcclxxiii

Was ist der AWS Control Tower?

AWS Control Tower bietet eine einfache Möglichkeit, eine Umgebung mit AWS mehreren Konten einzurichten und zu verwalten, wobei präskriptive Best Practices befolgt werden. AWS Control Tower orchestriert die Funktionen mehrerer anderer AWS Dienste, darunter, und AWS Organizations AWS Service Catalog AWS IAM Identity Center, um eine Landezone in weniger als einer Stunde einzurichten. Ressourcen werden in Ihrem Namen eingerichtet und verwaltet.

Die AWS Control Tower-Orchestrierung erweitert die Funktionen von AWS Organizations. Um zu verhindern, dass Ihre Organisationen und Konten von den bewährten Methoden abweichen, wendet der AWS Control Tower Kontrollen an (manchmal auch als Leitplanken bezeichnet). Beispielsweise können Sie mithilfe von Kontrollen sicherstellen, dass Sicherheitsprotokolle und die erforderlichen kontoübergreifenden Zugriffsberechtigungen erstellt und nicht geändert werden.

Wenn Sie mehr als eine Handvoll Konten hosten, ist es von Vorteil, über eine Orchestrierungsebene zu verfügen, die die Kontobereitstellung und Kontoverwaltung erleichtert. Sie können AWS Control Tower als Ihre primäre Methode zur Bereitstellung von Konten und Infrastruktur verwenden. Mit AWS Control Tower können Sie Unternehmensstandards einfacher einhalten, behördliche Anforderungen erfüllen und bewährte Verfahren befolgen.

Mit AWS Control Tower können Endbenutzer in Ihren verteilten Teams mithilfe konfigurierbarer Kontovorlagen in Account Factory schnell neue AWS Konten einrichten. In der Zwischenzeit können Ihre zentralen Cloud-Administratoren überwachen, ob alle Konten den etablierten, unternehmensweiten Compliance-Richtlinien entsprechen.

Kurz gesagt, AWS Control Tower bietet die einfachste Möglichkeit, eine sichere, konforme AWS Umgebung mit mehreren Konten einzurichten und zu verwalten, die auf bewährten Methoden basiert, die in der Zusammenarbeit mit Tausenden von Unternehmen entwickelt wurden. Weitere Informationen zur Arbeit mit AWS Control Tower und zu den bewährten Methoden, die in der Strategie für AWS mehrere Konten beschrieben sind, finden Sie unter. AWS Strategie für mehrere Konten: Leitfaden für bewährte Verfahren

Features

AWS Control Tower verfügt über die folgenden Funktionen:

- Landezone — Eine Landezone ist eine gut durchdachte Umgebung mit mehreren Konten, die auf bewährten Sicherheits- und Compliance-Methoden basiert. Es handelt sich um den

unternehmensweiten Container, der all Ihre Organisationseinheiten (OUs), Konten, Benutzer und anderen Ressourcen enthält, für die Sie Compliance-Vorschriften einhalten möchten. Landing Zones sind skalierbar, sodass sie den Anforderungen von Unternehmen aller Größen gerecht werden können.

- Kontrollen — Eine Kontrolle (manchmal auch als Leitplanke bezeichnet) ist eine übergeordnete Regel, die die kontinuierliche Steuerung Ihrer gesamten Umgebung gewährleistet. AWS Sie sind in Klartext. Es gibt drei Arten von Kontrollen: präventive , detektivische und proaktive. Für Kontrollen gelten drei Kategorien von Leitlinien: obligatorische, dringend empfohlene oder fakultative Kontrollen. Weitere Informationen zu Kontrollen finden Sie unterWie funktionieren Steuerungen.
- Account Factory — Eine Account Factory ist eine konfigurierbare Kontovorlage, mit deren Hilfe die Bereitstellung neuer Konten mit vorab genehmigten Kontokonfigurationen standardisiert werden kann. AWS Control Tower bietet eine integrierte Account Factory, mit der Sie den Workflow zur Kontobereitstellung in Ihrem Unternehmen automatisieren können. Weitere Informationen finden Sie unter Bereitstellung und Verwaltung von Konten mit Account Factory.
- Dashboard — Das Dashboard bietet Ihrem Team aus zentralen Cloud-Administratoren einen kontinuierlichen Überblick über Ihre Landing Zone. Verwenden Sie das Dashboard, um zu sehen, welche Konten in Ihrem Unternehmen bereitgestellt wurden, welche Kontrollen für die Durchsetzung von Richtlinien aktiviert sind, Kontrollen, die für die kontinuierliche Erkennung von Richtlinienverstößen aktiviert sind, und Ressourcen, die nicht den Richtlinien entsprechen, geordnet nach Konten und Organisationseinheiten.

Wie der AWS Control Tower mit anderen interagiert AWS service

AWS Control Tower basiert auf vertrauenswürdigen und zuverlässigen AWS Diensten wie AWS Service Catalog AWS IAM Identity Center, und AWS Organizations. Weitere Informationen finden Sie unter Integrierte Services.

Sie können AWS Control Tower zusammen mit anderen AWS Services in eine Lösung integrieren, die Sie bei der Migration Ihrer vorhandenen Workloads unterstützt. AWS Weitere Informationen finden Sie unter So nutzen Sie die Vorteile von AWS Control Tower und migrieren Workloads CloudEndure zu. AWS

Konfiguration, Steuerung und Erweiterbarkeit

- Automatisierte Kontokonfiguration: AWS Control Tower automatisiert die Bereitstellung und Registrierung von Konten mithilfe einer Account Factory (oder „Verkaufsautomat“), die

als Abstraktion auf den bereitgestellten Produkten aufgebaut ist. AWS Service Catalog Die Account Factory kann AWS Konten erstellen und registrieren und automatisiert den Prozess der Anwendung von Kontrollen und Richtlinien auf diese Konten. Weitere Informationen zum Erstellen und Bereitstellen von Konten finden Sie unter Bereitstellungsmethoden.

- Zentralisierte Verwaltung: Durch die Nutzung der Funktionen von richtet AWS Control Tower ein Framework ein AWS Organizations, das eine konsistente Compliance und Governance in Ihrer Umgebung mit mehreren Konten gewährleistet. Der AWS Organizations Service bietet wichtige Funktionen für die Verwaltung einer Umgebung mit mehreren Konten, einschließlich zentraler Steuerung und Verwaltung von Konten, Kontoerstellung über AWS Organizations APIs, Service Control Policies (SCPs) und Resource Control Policies (RCPs).

- Erweiterbarkeit: Sie können Ihre eigene AWS Control Tower-Umgebung erstellen oder erweitern AWS Organizations, indem Sie sowohl direkt in als auch in der AWS Control Tower-Konsole arbeiten. Sie können sehen, dass Ihre Änderungen im AWS Control Tower übernommen werden, nachdem Sie Ihre bestehenden Organisationen registriert und Ihre bestehenden Konten bei AWS Control Tower registriert haben. Sie können Ihre AWS Control Tower-Landezone aktualisieren, um Ihre Änderungen zu berücksichtigen. Wenn Ihre Workloads weitere erweiterte Funktionen erfordern, können Sie neben AWS Control Tower auch andere AWS Partnerlösungen nutzen.

Sind Sie ein First-Time Benutzer von AWS Control Tower?

Wenn Sie diesen Service zum ersten Mal verwenden, empfehlen wir Ihnen, Folgendes zu lesen:

1. Weitere Informationen zur Planung und Organisation Ihrer Landezone finden Sie unter Planen Sie Ihre AWS Control Tower Tower-Landezone undAWS Strategie für mehrere Konten für Ihre AWS Control Tower Tower-Landezone.
2. Wenn Sie zur Erstellung einer ersten Landing Zone bereit sind, finden Sie weitere Informationen unter Erste Schritte mit AWS Control Tower.
3. Informationen zur Erkennung und Vorbeugung von Abweichungen finden Sie unter Abweichungen im AWS Control Tower erkennen und beheben.
4. Sicherheitsdetails finden Sie unter Sicherheit im AWS Control Tower.
5. Informationen zur Aktualisierung Ihrer Landezone und Ihrer Mitgliedskonten finden Sie unterVerwaltung von Konfigurationsupdates in AWS Control Tower.

So funktioniert AWS Control Tower

In diesem Abschnitt wird ausführlich beschrieben, wie AWS Control Tower funktioniert. Ihre landing zone ist eine gut strukturierte Umgebung mit mehreren Konten für all Ihre Ressourcen. AWS Sie können diese Umgebung verwenden, um Compliance-Vorschriften für alle Ihre Konten durchzusetzen. AWS

Struktur einer AWS-Kontrollturm-Landezone

Die Struktur einer landing zone in AWS Control Tower sieht wie folgt aus:

- Root — Das übergeordnete Element, das alle anderen OUs in Ihrer landing zone enthält.
- Security OU — Wenn Sie Ihre landing zone starten, können Sie benutzerdefinierte Namen für Konten in der Security OU wählen und bestehende AWS Konten für Serviceintegrationen in AWS Control Tower übernehmen.

  In der AWS Control Tower landing zone Version 3.3 und früher enthält diese Organisationseinheit die Konten Log Archive und Audit. Diese Konten werden als gemeinsame Konten bezeichnet. In landing zone Version 3.3 und früher können Sie nach dem ersten Start keine vorhandenen Konten aus Sicherheits- und Protokollierungsgründen hinzufügen.

  In der AWS Control Tower landing zone Version 4.0 benötigt AWS Control Tower keine Sicherheits-OU mehr, und Sie können Ihre eigene Organisationsstruktur definieren.
- Sandbox-OU — Die Sandbox-OU wird erstellt, wenn Sie Ihre landing zone starten, sofern Sie sie aktivieren. Diese und andere registrierte Organisationseinheiten enthalten die registrierten Konten, mit denen Ihre Benutzer ihre Workloads ausführen. AWS
- IAM Identity Center-Verzeichnis — Dieses Verzeichnis enthält standardmäßig Ihre IAM Identity Center-Benutzer. Es definiert den Umfang der Berechtigungen für jeden IAM Identity Center-Benutzer. Optional können Sie sich dafür entscheiden, Ihre Identität und Zugriffskontrolle selbst zu verwalten. Weitere Informationen finden Sie unter Arbeiten mit AWS IAM Identity Center und AWS Control Tower.
- IAM Identity Center-Benutzer — Dies sind die Identitäten, von denen Ihre Benutzer annehmen können, um ihre AWS Workloads in Ihrer landing zone auszuführen.

Was passiert, wenn Sie eine landing zone einrichten

Wenn Sie eine landing zone einrichten, führt AWS Control Tower in Ihrem Namen die folgenden Aktionen in Ihrem Verwaltungskonto durch:

- Wenn Sie Ihre landing zone über die Konsole erstellen, erstellt AWS Control Tower zwei AWS Organizations Organisationseinheiten (OUs). Dies sind die Sicherheits-OU und die optionale Sandbox-OU, die in der organisatorischen Stammstruktur enthalten sind. Während der Einrichtung wählt AWS Control Tower automatisch die Sicherheits-OU als Standard-OU für Service-Integrationen aus. Diese OU wird als designierte Serviceintegrations-OU bezeichnet. Sie können bei der Einrichtung der landing zone eine andere Organisationseinheit auswählen.

  Für AWS Control Tower müssen sich alle für AWS Service-Integrationen konfigurierten Konten unter derselben OU befinden, die direkt unter Root verschachtelt ist. Diese Anforderung gilt nicht für das Verwaltungskonto.

  Wenn Sie Ihre landing zone über die API erstellen, wählen Sie nicht explizit eine OU für Serviceintegrationen aus. Serviceintegrationskonten müssen sich unter derselben OU befinden, die direkt unter dem Stammverzeichnis verschachtelt ist, und die Organisationseinheit, die Ihre Serviceintegrationskonten enthält, ist die designierte Serviceintegrations-OU. Weitere Informationen finden Sie unter Erste Schritte mit AWS Control Tower APIs.
- AWS Control Tower erstellt oder registriert Konten für alle aktivierten Service-Integrationen (wie AWS Config AWS CloudTrail, oder AWS Backup) in der angegebenen Service-Integrations-OU.
- Erstellt ein cloudnatives Verzeichnis in IAM Identity Center mit vorkonfigurierten Gruppen und Single Sign-On-Zugriff, wenn Sie die Standardkonfiguration von AWS Control Tower wählen, oder es ermöglicht Ihnen, Ihren Identitätsanbieter selbst zu verwalten.
- Wendet alle obligatorischen, präventiven Kontrollen an, um Richtlinien durchzusetzen.
- Wendet alle obligatorischen, detektiven Kontrollen an, um Verstöße gegen die Konfiguration zu erkennen.
- Präventive Kontrollen werden nicht auf das Verwaltungskonto angewendet.
- Mit Ausnahme des Verwaltungskontos gelten die Kontrollen für die gesamte Organisation.

Sichere Verwaltung von Ressourcen innerhalb Ihrer AWS Control Tower Landing Zone und Konten

- Wenn Sie Ihre landing zone erstellen, werden eine Reihe von AWS Ressourcen erstellt. Um AWS Control Tower verwenden zu können, dürfen Sie diese von AWS Control Tower verwalteten

Ressourcen nicht außerhalb der in diesem Handbuch beschriebenen unterstützten Methoden ändern oder löschen. Wenn Sie diese Ressourcen löschen oder ändern, wird Ihre landing zone in einen unbekannten Zustand versetzt. Details hierzu finden Sie unter Anleitung zur Erstellung und Änderung von AWS Control Tower Tower-Ressourcen

- Wenn Sie optionale Kontrollen aktivieren (solche mit dringend empfohlenen oder optionalen Anleitungen), erstellt AWS Control Tower AWS Ressourcen, die in Ihren Konten verwaltet werden. Ändern oder löschen Sie keine Ressourcen, die von AWS Control Tower erstellt wurden. Dies kann dazu führen, dass die Kontrollen in einen unbekannten Zustand übergehen.

Was sind die gemeinsamen Konten?

In AWS Control Tower werden die gemeinsamen Konten in Ihrer landing zone während der Einrichtung bereitgestellt: das Verwaltungskonto, das Protokollarchiv-Konto und das Audit-Konto.

Was ist das Verwaltungskonto?

Dies ist das Konto, das Sie speziell für Ihre landing zone erstellt haben. Dieses Konto wird für die Abrechnung von allem in Ihrer landing zone verwendet. Es wird auch für die Account Factory Factory-Bereitstellung von Konten sowie für die Verwaltung von Organisationseinheiten und Kontrollen verwendet.

> **Note**
>
> Es wird nicht empfohlen, Produktionsworkloads jeglicher Art von einem AWS Control Tower Tower-Managementkonto aus auszuführen. Erstellen Sie ein separates AWS Control Tower Tower-Konto, um Ihre Workloads auszuführen.

Weitere Informationen finden Sie unter Verwaltungskonto.

Was ist das Protokollarchiv-Konto?

Dieses Konto dient als Repository für Protokolle von API-Aktivitäten und Ressourcenkonfigurationen von allen Konten in der landing zone.

Weitere Informationen finden Sie unter CloudTrail Administratorkonto.

Was ist das Auditkonto?

Das Auditkonto ist ein eingeschränktes Konto, das Ihren Sicherheits- und Compliance-Teams Lese- und Schreibzugriff auf alle Konten in Ihrer landing zone. Über das Prüfungskonto haben Sie programmgesteuerten Zugriff auf Prüfkonten, indem Sie eine Rolle verwenden, die nur Lambda-Funktionen gewährt wird. Das Prüfungskonto erlaubt Ihnen nicht, sich manuell bei anderen Konten anzumelden. Weitere Informationen zu Lambda-Funktionen und -Rollen finden Sie unter Eine Lambda-Funktion so konfigurieren, dass sie eine Rolle von einer anderen übernimmt. AWS-Konto

Weitere Informationen finden Sie unter Aggregatorkonto konfigurieren.

Wie funktionieren Steuerungen

Eine Kontrolle ist eine Regel auf hoher Ebene, die eine kontinuierliche Steuerung Ihrer gesamten AWS Umgebung gewährleistet. Jede Kontrolle erzwingt eine einzige Regel, die in einfacher Sprache ausgedrückt wird. Sie können die ausgewählten oder dringend empfohlenen Kontrollen, die in Kraft sind, jederzeit über die AWS Control Tower Tower-Konsole oder die AWS Control Tower Tower-APIs ändern. Obligatorische Kontrollen werden immer angewendet und können nicht geändert werden.

Präventive Kontrollen verhindern, dass Maßnahmen ergriffen werden. Beispielsweise verhindert das optionale Steuerelement Disallow Changes to Bucket Policy for Amazon S3 Buckets (früher Disallow Policy Changes to Log Archive) jegliche Änderungen der IAM-Richtlinie innerhalb des gemeinsamen Logarchiv-Kontos. Jeder Versuch, eine verhinderte Aktion durchzuführen, wird verweigert und in CloudTrail protokolliert. Die Ressource ist auch angemeldet. AWS Config

Detective Controls erkennen bestimmte Ereignisse, wenn sie auftreten, und protokollieren die AktionCloudTrail. Das dringend empfohlene Steuerelement mit dem Namen „Erkennen, ob die Verschlüsselung für Amazon EBS-Volumes aktiviert ist, die an Amazon EC2 EC2-Instances angehängt sind“ erkennt beispielsweise, ob ein unverschlüsseltes Amazon EBS-Volume an eine EC2-Instance in Ihrer landing zone angehängt ist.

Proaktive Kontrollen überprüfen, ob die Ressourcen Ihren Unternehmensrichtlinien und -zielen entsprechen, bevor die Ressourcen Ihren Konten zugewiesen werden. Wenn die Ressourcen nicht den Vorschriften entsprechen, werden sie nicht bereitgestellt. Proaktive Kontrollen überwachen mithilfe von CloudFormation Vorlagen Ressourcen, die in Ihren Konten eingesetzt würden.

Für diejenigen, die damit vertraut sind AWS: In AWS Control Tower werden präventive Kontrollen mit Service Control Policies (SCPs) und Resource Control Policies (RCPs) implementiert. Detektivkontrollen werden mit AWS Config Regeln implementiert. Proaktive Kontrollen werden mit CloudFormation Hooks implementiert.

Verwandte Themen

- Abweichungen im AWS Control Tower erkennen und beheben

So funktioniert AWS Control Tower mit StackSets

AWS Control Tower verwendet standardmäßig CloudFormation StackSets die Einrichtung von Ressourcen in Ihren Konten. Jedes Stack-Set hat StackInstances die, die Konten entsprechen, und zwei AWS-Regionen pro Konto. AWS Control Tower stellt eine Stack-Set-Instance pro Konto und Region bereit.

AWS Control Tower wendet Updates auf bestimmte Konten an, und zwar AWS-Regionen selektiv, basierend auf CloudFormation Parametern. Wenn Aktualisierungen auf einige Stack-Instances angewendet werden, behalten andere Stack-Instances möglicherweise den Status Outdated (Veraltet) bei. Dieses Verhalten wird erwartet und ist normal.

Wenn eine Stack-Instance in den Status Outdated (Veraltet) wechselt, bedeutet dies normalerweise, dass der Stack, der dieser Stack-Instance entspricht, nicht mit der neuesten Vorlage im Stack-Set übereinstimmt. Der Stack verbleibt in der älteren Vorlage, daher enthält er möglicherweise nicht die neuesten Ressourcen oder Parameter. Der Stack ist immer noch vollständig nutzbar.

Im Folgenden finden Sie eine kurze Zusammenfassung des zu erwartenden Verhaltens auf der Grundlage der CloudFormation Parameter, die während eines Updates angegeben werden:

Wenn das Stack-Set-Update Änderungen an der Vorlage beinhaltet (d. h., wenn die `TemplateURL` Eigenschaften `TemplateBody` oder angegeben sind) oder wenn die `Parameters` Eigenschaft angegeben ist, CloudFormation markiert es alle Stack-Instances mit dem Status Veraltet, bevor die Stack-Instances in den angegebenen Konten aktualisiert werden und AWS-Regionen. Wenn das Stack-Set-Update keine Änderungen an der Vorlage oder den Parametern beinhaltet, werden die Stack-Instances in den angegebenen Konten und Regionen CloudFormation aktualisiert, während alle anderen Stack-Instances ihren bestehenden Stack-Instance-Status behalten. Damit alle Stack-Instances aktualisiert werden, die einem Stack-Set zugeordnet sind, geben Sie die Eigenschaft `Accounts` oder `Regions` nicht an.

Weitere Informationen finden Sie unter Aktualisieren Sie Ihr Stack-Set im CloudFormation Benutzerhandbuch.

Terminologie

Hier finden Sie einen kurzen Überblick über einige Begriffe, die Sie in der AWS Control Tower-Dokumentation finden werden.

Zunächst ist es gut zu wissen, dass der AWS Control Tower viele Begriffe mit dem AWS Organizations Service gemeinsam hat, einschließlich der Begriffe Organisation und Organisationseinheit (OU), die überall in diesem Dokument vorkommen.

- Weitere Informationen zu Organisationen und Organisationseinheiten finden Sie unter AWS Organizations Terminologie und Konzepte. Wenn Sie noch nicht mit AWS Control Tower vertraut sind, ist diese Terminologie ein guter Anfang.
- AWS Organizationsist ein AWS Service, der Ihnen hilft, Ihre Umgebung zentral zu verwalten, während Sie Ihre Workloads erweitern und skalieren. AWS AWS Control Tower stützt sich AWS Organizations auf die Erstellung von Konten, die Durchsetzung präventiver Kontrollen auf der Ebene der Organisationseinheiten und die zentrale Abrechnung.
- Ein AWS Account Factory-Konto ist ein AWS Konto, das mithilfe von Account Factory im AWS Control Tower bereitgestellt wird. Manchmal wird Account Factory informell als „Verkaufsautomat“ für Konten bezeichnet.
- Ihre AWS Control Tower-Heimatregion ist die AWS Region, in der Ihre AWS Control Tower-Landezone bereitgestellt wurde. Sie können Ihre Heimatregion in den Einstellungen Ihrer Landezone einsehen.
- AWS Service Catalogermöglicht es Ihnen, häufig eingesetzte IT-Services zentral zu verwalten. Im Zusammenhang mit diesem Dokument verwendet Account Factory AWS Service Catalog die Bereitstellung neuer AWS Konten, einschließlich Konten aus benutzerdefinierten Blueprints.
- AWS CloudFormation StackSetssind ein Ressourcentyp, der die Funktionalität von Stacks erweitert, sodass Sie Stacks für mehrere Konten und Regionen mit einem einzigen Vorgang und einer einzigen Vorlage erstellen, aktualisieren oder löschen können. CloudFormation
- Eine Stack-Instance ist eine Referenz auf einen Stack in einem Zielkonto innerhalb einer Region.
- Ein Stack ist eine Sammlung von AWS Ressourcen, die Sie als eine Einheit verwalten können.
- Ein Aggregator ist ein AWS Config Ressourcentyp, der AWS Config Konfigurations- und Compliance-Daten von mehreren Konten und Regionen innerhalb der Organisation sammelt, sodass Sie diese Compliance-Daten innerhalb eines einzigen Kontos anzeigen und abfragen können.

- Ein Konformitätspaket ist eine Sammlung von AWS Config Regeln und Abhilfemaßnahmen, die als einzelne Einheit in einem Konto und einer Region oder in einer gesamten Organisation in bereitgestellt werden können. AWS Organizations Sie können ein Conformance Pack verwenden, um Ihre AWS Control Tower-Umgebung anzupassen. Technische Blogs mit weiteren Informationen finden Sie unter Verwandte Informationen.
- Eine Basislinie in AWS Control Tower ist eine Gruppe von Ressourcen und spezifischen Konfigurationen, die Sie auf ein Ziel anwenden können. Das gängigste Basisziel kann eine Organisationseinheit (OU) sein. So `AWSControlTowerBaseline` steht beispielsweise der Baseline-Name zur Verfügung, um Ihnen bei der Registrierung Ihrer OUs bei AWS Control Tower zu helfen. Bei der Einrichtung und Aktualisierung der Landezone kann das Basisziel ein gemeinsames Konto oder eine bestimmte Einstellung für die gesamte Landezone sein.
- Blueprint: Ein Blueprint ist ein Artefakt, das einige Metadaten enthält, die Infrastrukturkomponenten beschreiben, die innerhalb eines Kontos bereitgestellt werden. Eine CloudFormation Vorlage kann beispielsweise als Entwurf für ein AWS Control Tower-Konto dienen.
- Drift: Eine Änderung einer Ressource, die von AWS Control Tower installiert und konfiguriert wurde. Ressourcen ohne Drift ermöglichen es dem AWS Control Tower, ordnungsgemäß zu funktionieren.
- Non-compliant Ressource: Eine Ressource, die gegen eine AWS Config Regel verstößt, die eine bestimmte Detektivkontrolle definiert.
- Gemeinsames Konto: Eines der drei Konten, die AWS Control Tower automatisch erstellt, wenn Sie Ihre Landing Zone einrichten: das Verwaltungskonto, das Log-Archiv-Konto und das Audit-Konto. Sie können bei der Einrichtung benutzerdefinierte Namen für das Protokollarchivkonto und das Auditkonto wählen.
- Mitgliedskonto: Ein Mitgliedskonto gehört der AWS Control Tower-Organisation. Das Mitgliedskonto kann bei AWS Control Tower registriert oder abgemeldet werden. Wenn eine registrierte OU eine Mischung aus registrierten und nicht registrierten Konten enthält:
  - Präventive Kontrollen, die in der OU aktiviert sind (oder von ihr übernommen wurden), gelten für alle darin enthaltenen Konten, auch für Konten, für die die OU nicht registriert ist. Das ist richtig, weil präventive Kontrollen mithilfe von SCPs, RCPS oder deklarativen Richtlinien auf Ebene der Organisationseinheit und nicht auf Kontoebene durchgesetzt werden. Weitere Informationen finden Sie in der Dokumentation unter Vererbung von Service Control-Richtlinien. AWS Organizations
  - Detective Controls, die in der OU aktiviert sind, gelten nicht für Konten, die nicht registriert sind.
  - Proaktive Kontrollen werden durch Hooks implementiert. AWS CloudFormation Diese Kontrollen gelten nicht für Konten, die in einer OU nicht registriert sind.

Ein Konto kann jeweils nur Mitglied einer Organisation sein, und seine Gebühren werden dem Verwaltungskonto dieser Organisation in Rechnung gestellt. Ein Mitgliedskonto kann in den Stammcontainer einer Organisation verschoben werden.

- AWS Konto: Ein AWS Konto fungiert als Ressourcencontainer und als Grenze zur Ressourcenisolierung. Ein AWS Konto kann mit Abrechnung und Zahlung verknüpft werden. Ein AWS Konto unterscheidet sich von einem Benutzerkonto (manchmal auch als IAM-Benutzerkonto bezeichnet) in AWS Control Tower. Konten, die im Rahmen des Account Factory-Bereitstellungsprozesses erstellt wurden, sind AWS Konten. AWS Konten können auch im Rahmen einer Kontoregistrierung oder einer OU-Registrierung zu AWS Control Tower hinzugefügt werden.
- Kontrolle: Eine Kontrolle (auch als Leitplanke bezeichnet) ist eine allgemeine Regel, die die kontinuierliche Steuerung Ihrer gesamten AWS Control Tower-Umgebung gewährleistet. Jede Kontrolle erzwingt eine einzelne Regel. Präventive Kontrollen werden mithilfe von Service Control Policies (SCPs), Resource Control Policies (RCPs) und deklarativen Richtlinien implementiert. Detektivkontrollen werden anhand von Regeln implementiert. AWS Config Proaktive Kontrollen werden mit CloudFormation Hooks implementiert. Weitere Informationen finden Sie unter Wie funktionieren Steuerungen.
- Kontrollkatalog: Der AWS Control Tower Control-Katalog ist das Kompendium aller Steuerungen, die über den AWS Control Tower in der Konsole und in den APIs verfügbar sind. Er wurde früher Control Library genannt. Wir haben die Terminologie an den Namen des Namespaces, controlcatalog, angepasst.
- Landezone: Eine Landing Zone ist eine Cloud-Umgebung, die einen empfohlenen Ausgangspunkt bietet, einschließlich Standardkonten, Kontostruktur, Netzwerk- und Sicherheitslayouts usw. Von einer Landing Zone aus können Sie Workloads bereitstellen, die Ihre Lösungen und Anwendungen nutzen.
- Framework: Ein Framework ist ein spezifischer regulatorischer Standard oder eine Branchenanforderung. In der Control Catalog-Ontologie wird ein Framework durch ein Standardsteuerelement dargestellt. Weitere Informationen finden Sie in der Übersicht über die Control Catalog-Ontologie.
- Verschachtelte Organisationseinheit: Eine verschachtelte Organisationseinheit in AWS Control Tower ist eine Organisationseinheit, die in einer anderen Organisationseinheit enthalten ist. Eine verschachtelte Organisationseinheit kann genau eine übergeordnete Organisationseinheit haben, und jedes Konto kann Mitglied genau einer Organisationseinheit sein. Verschachtelte Organisationseinheiten bilden eine Hierarchie. Wenn Sie eine Richtlinie an eine der Organisationseinheiten in der Hierarchie anhängen, fließt sie nach unten und wirkt sich auf alle

untergeordneten Organisationseinheiten und Konten aus. Eine verschachtelte OU-Hierarchie im AWS Control Tower kann maximal fünf Ebenen tief sein.

- Übergeordnete Organisationseinheit: Die Organisationseinheit, die sich unmittelbar über der aktuellen Organisationseinheit in der Hierarchie befindet. Jede Organisationseinheit kann genau eine übergeordnete Organisationseinheit haben.
- Untergeordnete Organisationseinheit: Jede Organisationseinheit, die in der Hierarchie unter der aktuellen Organisationseinheit liegt. Eine Organisationseinheit kann viele untergeordnete Organisationseinheiten haben.
- OU-Hierarchie: Im AWS Control Tower kann die Hierarchie der verschachtelten Organisationseinheiten bis zu fünf Ebenen umfassen. Die Reihenfolge der Verschachtelung wird als Ebenen bezeichnet. Die oberste Ebene der Hierarchie wird als Ebene 1 bezeichnet.
- Top-level OU: Eine OU der obersten Ebene ist jede OU, die sich direkt unter dem Stamm befindet, nicht der Stamm selbst. Die Wurzel wird nicht als OU betrachtet.
- Regiert: Eine regulierte Region wird in Ihrer Umgebung vom AWS Control Tower gemäß den von Ihrem Unternehmen festgelegten Governance-Richtlinien verwaltet und kontrolliert. Diese AWS-Regionen werden überwacht, um bewährte Verfahren und Unternehmensrichtlinien einzuhalten. Ihre Ressourcen in diesen Regionen sind geschützt, wenn Sie die Steuerung des AWS Control Tower aktivieren.
- Nicht reguliert: Regionen, für die der Status Nicht verwaltet angezeigt wird, werden nicht vom AWS Control Tower kontrolliert oder überwacht. Diese halten sich in der AWS-Regionen Regel nicht an dieselben Governance-Richtlinien, die der AWS Control Tower durchsetzt. Sie können Ressourcen in diesen Regionen erstellen, aber diese Ressourcen sind nicht durch die Kontrollen des AWS Control Tower geschützt.
- Abgelehnt: Eine verweigerte Region wird speziell von AWS Control Tower blockiert. In Ihrer AWS Control Tower-Umgebung können Sie dort keine Ressourcen bereitstellen AWS-Regionen.

Preisgestaltung

Für die Nutzung von AWS Control Tower fallen keine zusätzlichen Gebühren an. Sie zahlen nur für die von AWS Control Tower aktivierten AWS Dienste und die Dienste, die Sie in Ihrer Landezone nutzen. Beispielsweise zahlen Sie für Service Catalog für die Bereitstellung von Konten bei Account Factory und AWS CloudTrail für Ereignisse, die in Ihrer Landing Zone verfolgt werden. Informationen zu den Preisen und Gebühren im Zusammenhang mit AWS Control Tower finden Sie unter Preise für AWS Control Tower.

Wenn Sie kurzlebige Workloads von Konten im AWS Control Tower aus ausführen, kann es zu einem Anstieg der damit verbundenen Kosten kommen. AWS Config Weitere Details finden Sie unter AWS Config -Preise. Wenden Sie sich an Ihren AWS Kundenbetreuer, um genauere Informationen zur Verwaltung dieser Kosten zu erhalten. Weitere Informationen zur AWS Config Funktionsweise mit AWS Control Tower finden Sie unterÜberwachen Sie Ressourcenänderungen mit AWS Config.

Wenn Sie AWS CloudTrail Trails außerhalb von AWS Control Tower implementieren, können Sie sie mit AWS Control Tower verwenden. Es können jedoch doppelte Gebühren anfallen, wenn Sie sich auch für Trails anmelden, die vom AWS Control Tower verwaltet werden. Wir empfehlen nicht, externe Trails einzurichten, es sei denn, Sie haben spezielle Anforderungen. Wenn Sie sich bei der Einrichtung oder Aktualisierung der Landezone dafür entscheiden, dies zu tun, richtet AWS Control Tower für Sie im Verwaltungskonto einen CloudTrail Trail auf Organisationsebene ein und aktiviert ihn. Informationen zur CloudTrail Kostenverwaltung finden Sie unter Kosten verwalten CloudTrail .

Einrichtung

Folgen Sie vor der ersten Verwendung AWS Control Tower den Schritten in diesem Abschnitt, um ein AWS Konto zu erstellen und Ihr AWS Control Tower Verwaltungskonto zu schützen. Informationen zu zusätzlichen Einrichtungsaufgaben speziell für AWS Control Tower finden Sie unterErste Schritte mit AWS Control Tower.

Melden Sie sich an für AWS

Melde dich an für ein AWS-Konto

Um loszulegen AWS, benötigen Sie eine AWS-Konto. Informationen zum Erstellen eines AWS-Konto finden Sie unter Erste Schritte mit einem AWS-Konto im AWS -Kontenverwaltung Referenzhandbuch.

Wenn Sie sich für Amazon Web Services (AWS) registrieren, wird Ihr AWS Konto automatisch für alle Dienste in angemeldet AWS, einschließlich AWS Control Tower. Wenn Sie bereits ein AWS Konto haben, fahren Sie mit der nächsten Aufgabe fort. Wenn Sie noch kein AWS Konto haben, gehen Sie wie folgt vor, um eines zu erstellen.

Notieren Sie sich Ihre AWS Kontonummer, da Sie sie für andere Aufgaben benötigen.

> **Sicherheit für Ihre Konten**
>
> Weitere Hinweise zur Einrichtung von bewährten Methoden zum Schutz Ihrer AWS Control Tower Konten finden Sie in der AWS Organizations Dokumentation.
>
> - Bewährte Methoden für das Verwaltungskonto
> - Bewährte Verfahren für Mitgliedskonten

Nächster Schritt

Erste Schritte mit AWS Control Tower

Erste Schritte mit AWS Control Tower

Dieses Verfahren für die ersten Schritte richtet sich an AWS Control Tower-Administratoren. Folgen Sie diesem Verfahren, wenn Sie bereit sind, Ihre Landezone mithilfe der AWS Control Tower-Konsole oder der APIs einzurichten.

Wenn Sie derzeit AWS Kunde sind, aber AWS Control Tower noch nicht kennen, sollten Sie den genannten Abschnitt lesenPlanen Sie Ihre AWS Control Tower Tower-Landezone, bevor Sie fortfahren.

Themen

- AWS Control Tower-Kurzanleitung
- Voraussetzung: Automatisierte Überprüfungen Ihres Verwaltungskontos vor dem Start
- Einrichtung einer dedizierten Umgebung für Ihre Steuerungen
- Erste Schritte mit AWS Control Tower von der Konsole aus
- Erste Schritte mit AWS Control Tower mithilfe von APIs
- Nächste Schritte

AWS Control Tower-Kurzanleitung

Wenn Sie noch nicht mit AWS Control Tower vertraut sind AWS, können Sie die Schritte in diesem Abschnitt befolgen, um schnell mit AWS Control Tower zu beginnen. Wenn Sie es vorziehen, Ihre AWS Control Tower Tower-Umgebung sofort anzupassen, finden Sie weitere Informationen unterSchritt 2. Konfiguriere und starte deine Landezone.

> **Note**
>
> AWS Control Tower richtet kostenpflichtige Dienste wie Amazon AWS CloudTrail AWS Config CloudWatch, Amazon S3 und Amazon VPC ein. Bei der Nutzung dieser Dienste können Kosten anfallen, wie auf der Preisseite angegeben. Die AWS Verwaltungskonsole zeigt Ihnen die Nutzung aller kostenpflichtigen Dienste und die anfallenden Kosten. AWS Control Tower selbst verursacht keine zusätzlichen Kosten.

Bevor Sie beginnen

Die wichtigste Entscheidung, die Sie treffen müssen, bevor Sie mit dem Einrichtungsprozess beginnen, ist die Auswahl Ihrer Heimatregion. Ihre Heimatregion ist die AWS Region, in der Sie die meisten Ihrer Workloads ausführen oder die meisten Ihrer Daten speichern werden. Sie kann nicht mehr geändert werden, nachdem Sie Ihre AWS Control Tower Tower-Landezone eingerichtet haben. Weitere Informationen zur Auswahl einer Heimatregion finden Sie unterAdministrative Tipps für die Einrichtung der landing zone.

> **Note**
>
> Standardmäßig wählt AWS Control Tower die Region, in der Ihr Konto derzeit betrieben wird, als Ihre Heimatregion aus. Sie können Ihre aktuelle Region oben rechts auf dem Bildschirm Ihrer AWS Managementkonsole sehen.

Das Schnellstartverfahren setzt voraus, dass Sie die Standardwerte für die Ressourcen in Ihrer AWS Control Tower Tower-Umgebung akzeptieren. Viele dieser Optionen können später geändert werden. Einige einmalige Optionen sind im genannten Abschnitt aufgeführtErwartungen an die Konfiguration der Landezone.

Wenn Sie ein neues AWS Konto erstellt haben, erfüllt es automatisch die erforderlichen Voraussetzungen für die Einrichtung von AWS Control Tower. Sie können mit den folgenden Schritten fortfahren.

Schnellstart-Schritte

1. Melden Sie sich mit Ihren Administratoranmeldedaten bei der AWS Managementkonsole an.
2. Navigieren Sie zur AWS Control Tower Tower-Konsole unter https://console.aws.amazon.com/controltower.
3. Stellen Sie sicher, dass Sie in Ihrer gewünschten Heimatregion arbeiten.
4. Wählen Sie Enable AWS Control Tower.
5. Folgen Sie den Anweisungen in der Konsole und akzeptieren Sie alle Standardwerte. Wählen Sie bestehende Konten für Ihr Aggregator-Konto und CloudTrail Administratorkonto aus oder erstellen Sie neue Konten.
6. Überprüfen Sie Ihre Auswahl. Wählen Sie Enable AWS Control Tower.
7. AWS Control Tower benötigt etwa 30 Minuten, um alle Ressourcen in Ihrer landing zone einzurichten.

Eine detailliertere Version der Einrichtung von AWS Control Tower, einschließlich Möglichkeiten zur Anpassung Ihrer Umgebung, finden Sie in den nächsten Themen.

> **Note**
>
> Wenn Sie zum ersten Mal Kunde sind und auf ein Einrichtungsproblem stoßen, wenden Sie sich an den Support, um AWS Unterstützung bei der Diagnose zu erhalten.

Voraussetzung: Automatisierte Überprüfungen Ihres Verwaltungskontos vor dem Start

Bevor der AWS Control Tower die Landezone einrichtet, führt er automatisch eine Reihe von Prüfungen vor dem Start in Ihrem Konto durch. Für diese Prüfungen sind keine Maßnahmen Ihrerseits erforderlich. Dadurch wird sichergestellt, dass Ihr Verwaltungskonto für die Änderungen bereit ist, mit denen Ihre Landezone eingerichtet wird. Hier sind die Prüfungen, die der AWS Control Tower vor der Einrichtung einer Landezone durchführt:

- Die bestehenden Servicelimits für den AWS-Konto müssen ausreichen, damit AWS Control Tower gestartet werden kann. Weitere Informationen finden Sie unter Einschränkungen und Kontingente in AWS Control Tower.
- Sie AWS-Konto müssen die folgenden AWS Dienste abonniert haben:
  - Amazon Simple Storage Service (Amazon-S3)
  - Amazon Elastic Compute Cloud (Amazon EC2)
  - Amazon SNS
  - Amazon Virtual Private Cloud (Amazon VPC)
  - AWS CloudFormation
  - AWS CloudTrail
  - Amazon CloudWatch
  - AWS Config
  - AWS Identity and Access Management (ICH BIN)
  - AWS Lambda

> **Note**
>
> Standardmäßig haben alle Konten diese Services abonniert.

Überlegungen für AWS IAM Identity Center (IAM Identity Center) -Kunden

- Wenn AWS IAM Identity Center (IAM Identity Center) bereits eingerichtet ist, muss die Heimatregion des AWS Control Tower mit der IAM Identity Center-Region identisch sein. Wenn das IAM Identity Center jedoch in der Region USA Ost (Nord-Virginia) (us-east-1) eingerichtet ist, verwendet AWS Control Tower diese Instance unabhängig von der ausgewählten Heimatregion.
- IAM Identity Center kann nur im Verwaltungskonto einer Organisation installiert werden.
- Je nach der von Ihnen ausgewählten Identitätsquelle gelten für Ihr IAM Identity Center-Verzeichnis drei Optionen:
  - IAM Identity Center User Store: Wenn AWS Control Tower mit IAM Identity Center eingerichtet ist, erstellt AWS Control Tower Gruppen im IAM Identity Center-Verzeichnis und gewährt dem von Ihnen ausgewählten Benutzer den Zugriff auf diese Gruppen für Mitgliedskonten.
  - Active Directory: Wenn IAM Identity Center für AWS Control Tower mit Active Directory eingerichtet ist, verwaltet AWS Control Tower das IAM Identity Center-Verzeichnis nicht. Es weist Benutzern oder Gruppen keine neuen AWS Konten zu.
  - Externer Identitätsanbieter: Wenn IAM Identity Center for AWS Control Tower mit einem externen Identitätsanbieter (IdP) eingerichtet ist, erstellt AWS Control Tower Gruppen im IAM Identity Center-Verzeichnis und gewährt dem Benutzer, den Sie für Mitgliedskonten auswählen, Zugriff auf diese Gruppen. Sie können bei der Kontoerstellung in Account Factory einen vorhandenen Benutzer von Ihrem externen IdP angeben. AWS Control Tower gewährt diesem Benutzer Zugriff auf das neu veräußerte Konto, wenn Benutzer mit demselben Namen zwischen IAM Identity Center und dem externen IdP synchronisiert werden. Sie können auch Gruppen in Ihrem externen IdP erstellen, die den Namen der Standardgruppen im AWS Control Tower entsprechen. Wenn Sie diesen Gruppen Benutzer zuweisen, haben diese Benutzer Zugriff auf Ihre registrierten Konten.

Weitere Informationen zur Arbeit mit IAM Identity Center und AWS Control Tower finden Sie unter Wissenswertes über IAM Identity Center-Konten und AWS Control Tower

Überlegungen für AWS Config und AWS CloudTrail Kunden

- Für AWS-Konto kann der vertrauenswürdige Zugriff im Verwaltungskonto der Organisation nicht aktiviert AWS Config werden. Informationen zum Deaktivieren des vertrauenswürdigen Zugriffs finden Sie in der AWS Organizations Dokumentation zum Aktivieren oder Deaktivieren des vertrauenswürdigen Zugriffs.
- Wenn Sie in einem vorhandenen Konto, das Sie bei AWS Control Tower registrieren möchten, bereits einen AWS Config Recorder, einen Bereitstellungskanal oder eine Aggregation eingerichtet haben, müssen Sie diese Konfigurationen ändern oder entfernen, bevor Sie mit der Registrierung der Konten beginnen, nachdem Ihre Landing Zone eingerichtet wurde. Diese Vorabprüfung gilt nicht für das AWS Control Tower-Managementkonto beim Start der Landing Zone. Weitere Informationen finden Sie unter Konten registrieren, die bereits vorhanden sind AWS Config Ressourcen.
- Wenn Sie kurzlebige Workloads von Konten im AWS Control Tower aus ausführen, können Sie im Zusammenhang mit Config einen Anstieg der Kosten feststellen. AWS Weitere Informationen zur Verwaltung dieser Kosten erhalten Sie von Ihrem AWS Kundenbetreuer.
- Wenn Sie ein Konto bei AWS Control Tower registrieren, unterliegt Ihr Konto dem Tarif für die AWS CloudTrail AWS Control Tower-Organisation. Wenn Sie bereits einen CloudTrail Trail für das Konto eingerichtet haben, werden Ihnen möglicherweise doppelte Gebühren angezeigt, es sei denn, Sie löschen den bestehenden Trail für das Konto, bevor Sie es bei AWS Control Tower registrieren. Informationen zu Trails auf Organisationsebene und AWS Control Tower finden Sie unter. Preisgestaltung

> **Note**
>
> Beim Start müssen AWS Security Token Service (STS) -Endpunkte im Verwaltungskonto für alle vom AWS Control Tower verwalteten Regionen aktiviert werden. Andernfalls kann der Start während des Konfigurationsprozesses fehlschlagen.

Einrichtung einer dedizierten Umgebung für Ihre Steuerungen

Mit der AWS Control Tower Landing Zone 4.0 können Sie jetzt eine reine Kontrollumgebung erstellen, ohne eine vollständige Landezone implementieren zu müssen. Diese Bereitstellungsoption ist für Kunden konzipiert, die bereits über eine AWS-Organisation verfügen und sich auf die Einführung verwalteter Steuerungen über den AWS Control Tower Control Catalog konzentrieren möchten.

Themen

- Erste Schritte
- Überlegungen zur AWS-Konfiguration
- Implementierungsprozess
- Wichtige Hinweise

Erste Schritte

Sehen Sie sich zunächst den AWS Control Tower Control-Katalog von der Startseite aus an, um mehr über die verfügbaren verwalteten Kontrollen, die zugehörigen Compliance-Frameworks und Kontrollmetadaten zu erfahren. Um dieses Erlebnis auf dem AWS Control Tower zu ermöglichen, wählen Sie Ich habe eine bestehende Umgebung und möchte die AWS-managed Steuerelemente auf der Konsole aktivieren aus. Anschließend bestätigen Sie Ihre Heimatregion und wählen optional weitere regierte Regionen aus. Während der Einrichtung können Sie die automatische Kontoregistrierung aktivieren, wodurch sichergestellt wird, dass Konten automatisch die Steuerelemente und Konfigurationen von ihrer übergeordneten Organisationseinheit (OU) übernehmen, wenn sie zwischen Organisationseinheiten verschoben werden.

Überlegungen zur AWS-Konfiguration

Sie haben die Möglichkeit, sie AWS Config bei der Ersteinrichtung oder später nach Bedarf zu aktivieren. AWS Config ist erforderlich, wenn Sie beabsichtigen, Detective Controls in Ihrer Umgebung zu verwenden. Wenn Sie sich für die Aktivierung entscheiden AWS Config, müssen Sie ein Aggregatorkonto einrichten, um die Konfigurations- und Compliance-Daten zu sammeln. Sie können entweder ein vorhandenes Konto auswählen oder während der Einrichtung ein neues erstellen. Zu den zusätzlichen Optionen gehören die Konfiguration der AWS KMS Schlüsselverschlüsselung und die Angabe der Amazon S3-Protokollaufbewahrungsfristen für die Aufzeichnung.

Implementierungsprozess

Wenn Sie darauf verzichten AWS Config, ist Ihre Umgebung sofort bereit für präventive und proaktive Kontrollen im Control Catalog.

Wenn Sie jedoch bereit sind, Ihre erste Detective Control zu aktivieren, müssen Sie die AWS Config Aufzeichnung aktivieren, indem die neue Steuerung auf den Ziel-OUs aktiviert `ConfigBaseline` wird. Dies ist ein einmaliger Einrichtungsvorgang pro Organisationseinheit. Die AWS Config Preise

richten sich nach der Anzahl der Konten pro Organisationseinheit und der Ressourcen pro Konto pro AWS-Region.

Wichtige Hinweise

Durch die Erstellung einer AWS Control Tower-Umgebung wird eine vertrauensvolle Beziehung zu dieser Umgebung aufgebaut AWS Organizations, sodass Abweichungen erkannt und Änderungen an Konten und Organisationseinheiten nachverfolgt werden können. Während der Einrichtung erstellt der AWS Control Tower eine Landing Zone-Konfiguration, die als Grundlage für Ihre verwaltete Kontrollumgebung dient.

Informationen zum Erstellen Ihrer Umgebung für Steuerungen mithilfe von APIs finden Sie unter:. Erste Schritte mit AWS Control Tower mithilfe von APIs Beachten Sie, dass das Manifestfeld bei Landing Zone 4.0 jetzt optional ist.

Erste Schritte mit AWS Control Tower von der Konsole aus

Dieses Verfahren für die ersten Schritte richtet sich an AWS Control Tower-Administratoren. Folgen Sie diesem Verfahren, wenn Sie bereit sind, Ihre Landezone mithilfe der AWS Control Tower-Konsole einzurichten. Von Anfang bis Ende sollte es ungefähr eine halbe Stunde dauern. Dieses Verfahren erfordert einige Voraussetzungen und drei Hauptschritte.

Wenn Sie derzeit AWS Kunde sind, aber AWS Control Tower noch nicht kennen, sollten Sie den genannten Abschnitt lesenPlanen Sie Ihre AWS Control Tower Tower-Landezone, bevor Sie fortfahren.

Themen

- Erwartungen an die Konfiguration der Landezone
- Schritt 1: Erstellen Sie die E-Mail-Adressen für Ihr gemeinsames Konto
- Schritt 2. Konfiguriere und starte deine Landezone
- Schritt 3. Überprüfe die Landezone und richte sie ein

Erwartungen an die Konfiguration der Landezone

Die Einrichtung Ihrer AWS Control Tower-Landezone besteht aus mehreren Schritten. Bestimmte Aspekte Ihrer AWS Control Tower-Landezone sind konfigurierbar. Andere Optionen können nach der Einrichtung nicht mehr geändert werden.

Wichtige Elemente, die während der Einrichtung konfiguriert werden müssen

- Sie können die Namen Ihrer Organisationseinheiten auf oberster Ebene während der Einrichtung auswählen. Sie können die Namen der Organisationseinheiten auch ändern, nachdem Sie Ihre Landezone eingerichtet haben. Standardmäßig heißen die Organisationseinheiten der obersten Ebene Security und Sandbox. Weitere Informationen finden Sie unter Richtlinien für die Einrichtung einer gut strukturierten Umgebung.
- Während der Einrichtung können Sie benutzerdefinierte Namen für die von AWS Control Tower erstellten gemeinsamen Konten auswählen, die standardmäßig als CloudTrail Administrator - und Aggregator-Konto bezeichnet werden.

> **Note**
>
> In Landing Zone-Versionen vor 4.0 tragen diese Konten standardmäßig die Namen „Log Archive“ und „Audit“. Kunden, die frühere Versionen verwenden, sehen möglicherweise immer noch die ursprünglichen Namen.

- Während der Einrichtung können Sie optional vorhandene AWS Konten angeben, die AWS Control Tower als Prüf- und Protokollarchivierungskonten verwenden soll. Wenn Sie bestehende AWS Konten angeben möchten und diese Konten über vorhandene AWS Config Ressourcen verfügen, müssen Sie die vorhandenen AWS Config Ressourcen löschen, bevor Sie die Konten bei AWS Control Tower registrieren können. (Dies ist eine einmalige Auswahl.)
- Wenn Sie das System zum ersten Mal einrichten oder ein Upgrade auf die Landing Zone-Version 3.0 durchführen, können Sie wählen, ob Sie AWS Control Tower gestatten möchten, einen AWS CloudTrail Pfad auf Organisationsebene für Ihre Organisation einzurichten, oder Sie können sich von den Trails abmelden, die vom AWS Control Tower verwaltet werden, und Ihre eigenen CloudTrail Trails verwalten. Sie können sich bei jeder Aktualisierung Ihrer Landezone für Trails auf Organisationsebene, die vom AWS Control Tower verwaltet werden, an- oder abmelden.
- Sie können optional eine benutzerdefinierte Aufbewahrungsrichtlinie für Ihren Amazon S3-Log-Bucket und Ihren Log-Access-Bucket festlegen, wenn Sie Ihre Landing Zone einrichten oder aktualisieren.
- Sie können optional einen zuvor definierten Blueprint angeben, der für die Bereitstellung benutzerdefinierter Mitgliedskonten über die AWS Control Tower-Konsole verwendet werden soll. Sie können Konten später anpassen, falls Ihnen kein Blueprint zur Verfügung steht. Siehe Passen Sie Konten mit Account Factory Customization (AFC) an.

Konfigurationsentscheidungen, die nicht rückgängig gemacht werden können

- Sie können Ihre Heimatregion nicht mehr ändern, nachdem Sie Ihre Landezone eingerichtet haben.
- Wenn Sie Account Factory-Konten mit VPCs einrichten, können VPC-CIDRs nicht mehr geändert werden, nachdem sie erstellt wurden.

Schritt 1: Erstellen Sie die E-Mail-Adressen für Ihr gemeinsames Konto

Wenn Sie Ihre Landezone in einer neuen einrichten AWS-Konto, finden Sie weitere Informationen unterEinrichtung.

- Um Ihre Landezone mit neuen gemeinsamen Konten einzurichten, benötigt AWS Control Tower zwei eindeutige E-Mail-Adressen, die noch nicht mit einem verknüpft sind AWS-Konto. Jede dieser E-Mail-Adressen dient als gemeinschaftlicher Posteingang — ein gemeinsames E-Mail-Konto —, das für die verschiedenen Benutzer in Ihrem Unternehmen bestimmt ist, die bestimmte Aufgaben im Zusammenhang mit AWS Control Tower erledigen werden.
- Wenn Sie AWS Control Tower zum ersten Mal einrichten und vorhandene Sicherheits- und Protokollarchivkonten in den AWS Control Tower integrieren, können Sie die aktuellen E-Mail-Adressen der vorhandenen AWS Konten eingeben.

Die E-Mail-Adressen sind erforderlich für:

- Auditkonto — Dieses Konto ist für Ihr Benutzerteam bestimmt, das Zugriff auf die vom AWS Control Tower zur Verfügung gestellten Auditinformationen benötigt. Sie können dieses Konto auch als Zugriffspunkt für Tools von Drittanbietern verwenden, die eine programmatische Prüfung der Umgebung auf Konformität durchführt
- Log-Archiv-Konto — Dieses Konto ist für Ihr Team von Benutzern bestimmt, die Zugriff auf alle Logging-Informationen für all Ihre registrierten Konten innerhalb registrierter OUs in Ihrer Landing Zone benötigen.

Diese Konten werden in der Security OU eingerichtet, wenn Sie Ihre Landing Zone erstellen. Als bewährte Methode empfehlen wir, dass Sie beim Ausführen von Aktionen in diesen Konten einen IAM Identity Center-Benutzer mit den entsprechenden Berechtigungen verwenden.

> **Note**
>
> Wenn Sie bestehende AWS Konten als Ihre Konten für Audit - und Protokollarchivierung angeben, müssen die vorhandenen Konten vor dem Start einige Prüfungen bestehen, um sicherzustellen, dass keine Ressourcen im Widerspruch zu den Anforderungen des AWS Control Tower stehen. Wenn diese Prüfungen nicht erfolgreich sind, ist die Einrichtung Ihrer Landezone möglicherweise nicht erfolgreich. Insbesondere dürfen die Konten keine vorhandenen AWS Config Ressourcen haben. Weitere Informationen finden Sie unter Überlegungen zur Verwendung vorhandener Sicherheits- oder Protokollkonten.

Der Übersichtlichkeit halber werden in diesem Benutzerhandbuch die gemeinsamen Konten immer mit ihren Standardnamen bezeichnet: Log-Archiv und Audit. Denken Sie beim Lesen dieses Dokuments daran, die benutzerdefinierten Namen, die Sie diesen Konten ursprünglich gegeben haben, zu ersetzen, falls Sie sie anpassen möchten. Sie können Ihre Konten mit ihren benutzerdefinierten Namen auf der Seite mit den Kontodetails einsehen.

> **Note**
>
> Wir ändern unsere Terminologie in Bezug auf die Standardnamen einiger AWS Control Tower-Organisationseinheiten (OUs), um sie an die Strategie mit AWS mehreren Konten anzupassen. Möglicherweise stellen Sie während der Umstellung einige Inkonsistenzen fest, um die Übersichtlichkeit dieser Namen zu verbessern. Die Security OU wurde früher Core OU genannt. Die Sandbox-Organisationseinheit wurde früher als benutzerdefinierte Organisationseinheit bezeichnet.

Schritt 2. Konfiguriere und starte deine Landezone

Bevor Sie Ihre AWS Control Tower-Landezone starten, ermitteln Sie die am besten geeignete Heimatregion. Weitere Informationen finden Sie unter Administrative Tipps für die Einrichtung der landing zone.

> **Important**
>
> Um Ihre Heimatregion zu ändern, nachdem Sie Ihre AWS Control Tower-Landezone eingerichtet haben, ist eine Außerbetriebnahme sowie die Unterstützung durch den AWS Support erforderlich. Diese Vorgehensweise wird nicht empfohlen.

Erfahren Sie, wie Sie Ihre Landing Zone mithilfe des AWS CLI Links konfigurieren und starten. Erste Schritte mit AWS Control Tower mithilfe von APIs

Gehen Sie wie folgt vor, um Ihre Landezone in der Konsole zu konfigurieren und zu starten.

Vorbereiten: Navigieren Sie zur AWS Control Tower-Konsole

1. Öffnen Sie einen Webbrowser und navigieren Sie zur AWS Control Tower-Konsole unter https://console.aws.amazon.com/controltower.
2. Vergewissern Sie sich in der Konsole, dass Sie in Ihrer gewünschten Heimatregion für AWS Control Tower arbeiten. Wählen Sie dann Ihre Landezone einrichten aus.

Schritt 2a. Überprüfen Sie und wählen Sie Ihre AWS Regionen

Vergewissern Sie sich, dass Sie die AWS Region, die Sie für Ihre Heimatregion ausgewählt haben, korrekt angegeben haben. Nachdem Sie den AWS Control Tower bereitgestellt haben, können Sie die Heimatregion nicht mehr ändern.

In diesem Abschnitt des Einrichtungsprozesses können Sie alle weiteren AWS Regionen hinzufügen, die Sie benötigen. Sie können bei Bedarf zu einem späteren Zeitpunkt weitere Regionen hinzufügen und Regionen aus der Verwaltung entfernen.

Um weitere auszuwählen AWS Zu regierende Regionen

1. Das Fenster zeigt Ihnen die aktuelle Regionsauswahl. Öffnen Sie das Drop-down-Menü, um eine Liste mit weiteren Regionen anzuzeigen, die für die Steuerung verfügbar sind.
2. Markieren Sie das Kästchen neben jeder Region, um die Verwaltung durch den AWS Control Tower zu aktivieren. Die Auswahl Ihrer Heimatregion kann nicht bearbeitet werden.

Um den Zugriff auf bestimmte Regionen zu verweigern

Um den Zugriff auf AWS Ressourcen und Workloads in bestimmten AWS Regionen zu verweigern, wählen Sie im Abschnitt „Region verweigern“ die Option Aktiviert aus. Die Standardeinstellung für dieses Steuerelement ist Nicht aktiviert.

Schritt 2b. Konfigurieren Sie Ihre Organisationseinheiten (OUs)

Wenn Sie die Standardnamen dieser OUs akzeptieren, müssen Sie keine Maßnahmen ergreifen, damit die Einrichtung fortgesetzt werden kann. Um die Namen der Organisationseinheiten zu ändern, geben Sie die neuen Namen direkt in das Formularfeld ein.

- Grundlegende Organisationseinheit — AWS Control Tower stützt sich auf eine grundlegende Organisationseinheit, die ursprünglich als Security OU bezeichnet wurde. Sie können den Namen dieser OU bei der Ersteinrichtung und danach auf der Seite mit den OU-Details ändern. Diese Sicherheitseinheit enthält Ihre beiden gemeinsamen Konten, die standardmäßig als Protokollarchivkonto und Auditkonto bezeichnet werden.
- Zusätzliche Organisationseinheit — AWS Control Tower kann eine oder mehrere zusätzliche Organisationseinheiten für Sie einrichten. Wir empfehlen, dass Sie neben der Sicherheits-OU mindestens eine zusätzliche OU in Ihrer Landing Zone bereitstellen. Wenn diese zusätzliche Organisationseinheit für Entwicklungsprojekte vorgesehen ist, empfehlen wir, ihr den Namen Sandbox-Organisationseinheit zu geben, wie in. Richtlinien für die Einrichtung einer gut strukturierten Umgebung Wenn Sie bereits über eine bestehende Organisationseinheit verfügen AWS Organizations, wird Ihnen möglicherweise die Option angezeigt, die Einrichtung einer zusätzlichen Organisationseinheit im AWS Control Tower zu überspringen.

Schritt 2c. Konfigurieren Sie Ihre gemeinsamen Konten, Protokollierung und Verschlüsselung

In diesem Abschnitt des Einrichtungsvorgangs werden im Bereich die Standardauswahlen für die Namen Ihrer gemeinsam genutzten AWS Control Tower-Konten angezeigt. Diese Konten sind ein wesentlicher Bestandteil Ihrer Landezone. Verschiebe oder lösche diese geteilten Konten nicht. Sie können bei der Einrichtung benutzerdefinierte Namen für die Audit - und Log-Archiv-Konten wählen. Alternativ haben Sie die einmalige Option, vorhandene AWS Konten als Ihre gemeinsamen Konten anzugeben.

Sie müssen eindeutige E-Mail-Adressen für Ihr Protokollarchiv und Ihre Auditkonten angeben, und Sie können die E-Mail-Adresse überprüfen, die Sie zuvor für Ihr Verwaltungskonto angegeben haben. Wählen Sie die Schaltfläche „Bearbeiten“, um die bearbeitbaren Standardwerte zu ändern.

Über die gemeinsamen Konten

- Das Verwaltungskonto — Das AWS Control Tower-Verwaltungskonto ist Teil der Root-Ebene. Das Verwaltungskonto ermöglicht die Abrechnung im AWS Control Tower. Das Konto verfügt auch über Administratorberechtigungen für Ihre Landezone. Sie können im AWS Control Tower keine separaten Konten für die Abrechnung und für Administratorberechtigungen erstellen.

  Die für das Verwaltungskonto angezeigte E-Mail-Adresse kann in dieser Phase der Einrichtung nicht bearbeitet werden. Sie wird als Bestätigung angezeigt, sodass Sie überprüfen können, ob Sie das richtige Verwaltungskonto bearbeiten, falls Sie mehrere Konten haben.
- Die beiden gemeinsamen Konten — Sie können benutzerdefinierte Namen für diese beiden Konten wählen oder Ihre eigenen Konten verwenden. Sie müssen für jedes neue oder bestehende Konto eine eindeutige E-Mail-Adresse angeben. Wenn Sie sich dafür entscheiden, dass AWS Control Tower neue gemeinsame Konten für Sie erstellt, dürfen den E-Mail-Adressen noch keine AWS Konten zugeordnet sein.

Geben Sie die angeforderten Informationen ein, um die gemeinsamen Konten zu konfigurieren.

1. Geben Sie an der Konsole einen Namen für das Konto ein, das ursprünglich als Protokollarchivkonto bezeichnet wurde. Viele Kunden entscheiden sich dafür, den Standardnamen für dieses Konto beizubehalten.
2. Geben Sie eine eindeutige E-Mail-Adresse für dieses Konto an.
3. Geben Sie einen Namen für das Konto ein, das ursprünglich als Auditkonto bezeichnet wurde. Viele Kunden nennen es das Sicherheitskonto.
4. Geben Sie eine eindeutige E-Mail-Adresse für dieses Konto an.

Konfigurieren Sie optional die Aufbewahrung von Protokollen

Während dieser Phase der Einrichtung können Sie die Richtlinie zur Aufbewahrung von Protokollen für Amazon S3-Buckets, die Ihre AWS CloudTrail Protokolle im AWS Control Tower speichern, in Schritten von Tagen oder Jahren, bis zu einem Maximum von 15 Jahren, anpassen. Wenn Sie Ihre Protokollspeicherung nicht anpassen möchten, sind die Standardeinstellungen ein Jahr für die Standardkontoprotokollierung und 10 Jahre für die Zugriffsprotokollierung. Diese Funktion ist auch verfügbar, wenn du deine Landezone aktualisierst oder zurücksetzt.

Optionale Selbstverwaltung AWS-Konto access

Sie können wählen, ob AWS Control Tower den AWS-Konto Zugriff mit AWS Identity and Access Management (IAM) einrichtet oder ob Sie den AWS-Konto Zugriff selbst verwalten möchten — entweder mit AWS IAM Identity Center-Benutzern, Rollen und Berechtigungen, die Sie selbst einrichten und anpassen können, oder mit einer anderen Methode wie einem externen IdP, entweder für den direkten Kontoverbund oder für den Verbund mehrerer Konten über IAM Identity Center. Sie können diese Auswahl später ändern.

Standardmäßig richtet AWS Control Tower das AWS IAM Identity Center für Ihre Landezone ein. Dabei werden die Empfehlungen zu bewährten Methoden befolgt, die unter Organisieren Ihrer AWS Umgebung mit mehreren Konten definiert sind. Die meisten Kunden wählen die Standardeinstellung. Manchmal sind alternative Zugriffsmethoden erforderlich, um gesetzliche Vorschriften in bestimmten Branchen oder Ländern einzuhalten oder AWS-Regionen wenn AWS IAM Identity Center nicht verfügbar ist.

Die Auswahl von Identitätsanbietern auf Kontoebene wird nicht unterstützt. Diese Option gilt nur für die gesamte Landezone.

Weitere Informationen finden Sie unter Anleitung zum IAM Identity Center.

Konfigurieren Sie optional AWS CloudTrail Trails

Als bewährte Methode empfehlen wir, die Protokollierung einzurichten. Wenn Sie möchten, dass AWS Control Tower einen CloudTrail Trail auf Organisationsebene einrichtet und für Sie verwaltet, wählen Sie Opt in. Wenn Sie die Protokollierung mit Ihren eigenen CloudTrail Trails oder einem Logging-Tool eines Drittanbieters verwalten möchten, wählen Sie Opt out. Bestätigen Sie Ihre Auswahl, wenn Sie in der Konsole dazu aufgefordert werden. Du kannst deine Auswahl ändern und Trails auf Organisationsebene aktivieren oder deaktivieren, wenn du deine Landezone aktualisierst.

Du kannst jederzeit deine eigenen CloudTrail Trails einrichten und verwalten, einschließlich Trails auf Organisations- und Kontoebene. Wenn du doppelte CloudTrail Trails einrichtest, können dir doppelte Kosten entstehen, wenn Ereignisse protokolliert werden. CloudTrail

Konfigurieren Sie optional AWS KMS keys

Wenn Sie Ihre Ressourcen mit einem AWS KMS Verschlüsselungsschlüssel verschlüsseln und entschlüsseln möchten, aktivieren Sie das Kontrollkästchen. Wenn Sie bereits Schlüssel haben, können Sie diese aus den Kennungen auswählen, die in einem Dropdownmenü angezeigt werden.

Sie können einen neuen Schlüssel generieren, indem Sie Schlüssel erstellen wählen. Sie können einen KMS-Schlüssel jederzeit hinzufügen oder ändern, wenn Sie Ihre Landezone aktualisieren.

Wenn Sie Landezone einrichten auswählen, führt AWS Control Tower eine Vorabprüfung durch, um Ihren KMS-Schlüssel zu validieren. Der Schlüssel muss die folgenden Anforderungen erfüllen:

- Aktiviert
- Symmetrisch
- Kein Schlüssel für mehrere Regionen
- Der Richtlinie wurden die richtigen Berechtigungen hinzugefügt
- Der Schlüssel befindet sich im Verwaltungskonto

Möglicherweise wird ein Fehlerbanner angezeigt, wenn der Schlüssel diese Anforderungen nicht erfüllt. Wählen Sie in diesem Fall einen anderen Schlüssel oder generieren Sie einen Schlüssel. Achten Sie darauf, die Berechtigungsrichtlinie des Schlüssels zu bearbeiten, wie im nächsten Abschnitt beschrieben.

Aktualisieren Sie die KMS-Schlüsselrichtlinie

Bevor Sie eine KMS-Schlüsselrichtlinie aktualisieren können, müssen Sie einen KMS-Schlüssel erstellen. Weitere Informationen finden Sie unter Erstellen einer Schlüsselrichtlinie im AWS Key Management Service -Entwicklerhandbuch.

Um einen KMS-Schlüssel mit AWS Control Tower zu verwenden, müssen Sie die standardmäßige KMS-Schlüsselrichtlinie aktualisieren, indem Sie die erforderlichen Mindestberechtigungen für AWS Config und hinzufügen AWS CloudTrail. Als bewährte Methode empfehlen wir, dass Sie die erforderlichen Mindestberechtigungen in jede Richtlinie aufnehmen. Wenn Sie eine KMS-Schlüsselrichtlinie aktualisieren, können Sie Berechtigungen als Gruppe in einer einzelnen JSON-Anweisung oder Zeile für Zeile hinzufügen.

Das Verfahren beschreibt, wie die standardmäßige KMS-Schlüsselrichtlinie in der AWS KMS Konsole aktualisiert wird, indem Richtlinienanweisungen hinzugefügt werden, die Verschlüsselung zulassen AWS Config und CloudTrail AWS KMS für diese verwendet werden können. Die Richtlinienanweisungen erfordern, dass Sie die folgenden Informationen angeben:

- **`YOUR-MANAGEMENT-ACCOUNT-ID`**— die ID des Verwaltungskontos, in dem AWS Control Tower eingerichtet wird.

- **YOUR-HOME-REGION**— die Heimatregion, die Sie bei der Einrichtung von AWS Control Tower auswählen werden.
- **YOUR-KMS-KEY-ID**— die KMS-Schlüssel-ID, die mit der Richtlinie verwendet wird.
- **PARTITION**— die Partition der AWS Region, in der Sie den AWS Control Tower eingerichtet haben, z. B. `awsaws-us-gov`,`aws-cn`, oder`aws-eusc`.

Um die KMS-Schlüsselrichtlinie zu aktualisieren

1. Öffnen Sie die AWS KMS Konsole unter https://console.aws.amazon.com/kms
2. Wählen Sie im Navigationsbereich die Option Kundenverwaltete Schlüssel aus.
3. Wählen Sie in der Tabelle den Schlüssel aus, den Sie bearbeiten möchten.
4. Vergewissern Sie sich, dass Sie auf der Registerkarte Schlüsselrichtlinie die Schlüsselrichtlinie einsehen können. Wenn Sie die wichtigste Richtlinie nicht anzeigen können, wählen Sie Zur Richtlinienansicht wechseln.
5. Wählen Sie „Bearbeiten“ und aktualisieren Sie die standardmäßige KMS-Schlüsselrichtlinie, indem Sie die folgenden Richtlinienanweisungen für AWS Config und hinzufügen CloudTrail.

   AWS Config Grundsatzerklärung

```
{
    "Sid": "Allow Config to use KMS for encryption",
    "Effect": "Allow",
    "Principal": {
        "Service": "config.amazonaws.com"
    },
    "Action": [
        "kms:Decrypt",
        "kms:GenerateDataKey"
    ],
    "Resource": "arn:PARTITION:kms:YOUR-HOME-REGION:YOUR-MANAGEMENT-ACCOUNT-
ID:key/YOUR-KMS-KEY-ID"
}
```

   CloudTrail politische Erklärung

```
{
    "Sid": "Allow CloudTrail to use KMS for encryption",
    "Effect": "Allow",
```

```
    "Principal": {
        "Service": "cloudtrail.amazonaws.com"
    },
    "Action": [
        "kms:GenerateDataKey*",
        "kms:Decrypt"
    ],
    "Resource": "arn:PARTITION:kms:YOUR-HOME-REGION:YOUR-MANAGEMENT-ACCOUNT-
ID:key/YOUR-KMS-KEY-ID",
    "Condition": {
        "StringEquals": {
            "aws:SourceArn": "arn:PARTITION:cloudtrail:YOUR-HOME-REGION:YOUR-
MANAGEMENT-ACCOUNT-ID:trail/aws-controltower-BaselineCloudTrail"
        },
        "StringLike": {
            "kms:EncryptionContext:aws:cloudtrail:arn":
 "arn:PARTITION:cloudtrail:*:YOUR-MANAGEMENT-ACCOUNT-ID:trail/*"
        }
    }
}
```

6. Wählen Sie Änderungen speichern aus.

Beispiel für eine KMS-Schlüsselrichtlinie

Die folgende Beispielrichtlinie zeigt, wie Ihre KMS-Schlüsselrichtlinie aussehen könnte, nachdem Sie die Richtlinienanweisungen hinzugefügt haben, CloudTrail die die erforderlichen Mindestberechtigungen gewähren AWS Config . Die Beispielrichtlinie beinhaltet nicht Ihre standardmäßige KMS-Schlüsselrichtlinie.

```
{
    "Version": "2012-10-17",
    "Id": "CustomKMSPolicy",
    "Statement": [
        {
        ... YOUR-EXISTING-POLICIES ...
        },
        {
            "Sid": "Allow Config to use KMS for encryption",
            "Effect": "Allow",
            "Principal": {
                "Service": "config.amazonaws.com"
            },
```

```
            "Action": [
                "kms:Decrypt",
                "kms:GenerateDataKey"
            ],
            "Resource": "arn:PARTITION:kms:YOUR-HOME-REGION:YOUR-MANAGEMENT-ACCOUNT-
ID:key/YOUR-KMS-KEY-ID"
        },
        {
            "Sid": "Allow CloudTrail to use KMS for encryption",
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudtrail.amazonaws.com"
            },
            "Action": [
                "kms:GenerateDataKey*",
                "kms:Decrypt"
              ],
            "Resource": "arn:PARTITION:kms:YOUR-HOME-REGION:YOUR-MANAGEMENT-ACCOUNT-
ID:key/YOUR-KMS-KEY-ID",
            "Condition": {
                "StringEquals": {
                    "aws:SourceArn": "arn:PARTITION:cloudtrail:YOUR-HOME-REGION:YOUR-
MANAGEMENT-ACCOUNT-ID:trail/aws-controltower-BaselineCloudTrail"
                },
                "StringLike": {
                    "kms:EncryptionContext:aws:cloudtrail:arn":
 "arn:PARTITION:cloudtrail:*:YOUR-MANAGEMENT-ACCOUNT-ID:trail/*"
                }
            }
        }
    ]
}
```

Weitere Beispielrichtlinien finden Sie auf den folgenden Seiten:

- Erteilen von Verschlüsselungsberechtigungen im AWS CloudTrail Benutzerhandbuch.
- Erforderliche Berechtigungen für den KMS-Schlüssel bei Verwendung von Service-Linked RolesS3 (Bucket Delivery) im AWS Config Entwicklerhandbuch.

> **Schützen Sie sich vor Angreifern**
>
> Indem Sie Ihren Richtlinien bestimmte Bedingungen hinzufügen, können Sie dazu beitragen, eine bestimmte Art von Angriff zu verhindern, den sogenannten Confused Deputy Attack, der auftritt, wenn eine Entität eine Entität mit mehr Rechten zu einer Aktion zwingt, z. B. durch dienstübergreifenden Identitätswechsel. Allgemeine Informationen zu den Richtlinienbedingungen finden Sie auch unter. Angeben von Bedingungen in einer Richtlinie

Mit AWS Key Management Service (AWS KMS) können Sie KMS-Schlüssel und asymmetrische Schlüssel für mehrere Regionen erstellen. AWS Control Tower unterstützt jedoch keine Schlüssel für mehrere Regionen oder asymmetrische Schlüssel. AWS Control Tower führt eine Vorabprüfung Ihrer vorhandenen Schlüssel durch. Möglicherweise wird eine Fehlermeldung angezeigt, wenn Sie einen Schlüssel für mehrere Regionen oder einen asymmetrischen Schlüssel auswählen. Generieren Sie in diesem Fall einen weiteren Schlüssel zur Verwendung mit AWS Control Tower-Ressourcen.

Weitere Informationen AWS KMS dazu finden Sie im AWS KMS Entwicklerhandbuch.

Beachten Sie, dass Kundendaten im AWS Control Tower im Ruhezustand standardmäßig mit verschlüsselt werden SSE-S3.

Konfigurieren Sie optional die automatische Registrierung für Konten

Wenn Sie diese Funktion während der Einrichtung oder später aktivieren, zeigen Konten, die zwischen zwei registrierten Organisationseinheiten verschoben oder zum ersten Mal in Ihre AWS Control Tower-Umgebung verschoben werden, keinen Vererbungsstatus mehr. Die Konten erben automatisch die Baselines und Steuerelemente, die in der neuen OU aktiviert sind. Steuerelemente und Baselines aus der vorherigen OU werden entfernt.

Um die automatische Registrierung jederzeit nach der Einrichtung zu aktivieren, navigieren Sie zur Seite mit den Landingzone-Einstellungen und wählen Sie Landing Zone aktualisieren aus, oder rufen Sie die AWS Control Tower API auf. `UpdateLandingZone`

Sie können ein Konto mithilfe der AWS Organizations API oder mithilfe der AWS Control Tower-Konsole zwischen Organisationseinheiten verschieben. Wenn Sie ein Konto außerhalb einer registrierten OU verschieben, entfernt AWS Control Tower automatisch alle bereitgestellten Baselines und Kontrollen. Das Konto wird im Wesentlichen vom AWS Control Tower abgemeldet.

> **Note**
>
> Wenn Sie sich nach der ersten Einrichtung der Landing Zone dafür entscheiden, die automatische Registrierung zu aktivieren, behebt AWS Control Tower die Vererbungsabweichung nicht rückwirkend, die durch das Verschieben von Konten zwischen Organisationseinheiten verursacht wurde, bevor die Funktion zur automatischen Registrierung aktiviert wurde. Die automatische Drift-Auflösung tritt für Konten in Kraft, die verschoben werden, nachdem Sie diese Einstellung aktiviert haben.

Konfigurieren und erstellen Sie optional benutzerdefinierte Mitgliedskonten

Wenn Sie dem Workflow „Konto erstellen“ folgen, um Ihre Mitgliedskonten hinzuzufügen, können Sie optional einen zuvor definierten Blueprint angeben, der für die Bereitstellung benutzerdefinierter Mitgliedskonten über die AWS Control Tower-Konsole verwendet werden soll. Sie können Konten später anpassen, falls Ihnen kein Blueprint zur Verfügung steht. Siehe Passen Sie Konten mit Account Factory Customization (AFC) an.

Schritt 3. Überprüfe die Landezone und richte sie ein

Der nächste Abschnitt in der Einrichtung zeigt Ihnen die Berechtigungen, die AWS Control Tower für Ihre Landezone benötigt. Wählen Sie ein Kontrollkästchen aus, um jedes Thema zu erweitern. Du wirst aufgefordert, diesen Genehmigungen zuzustimmen, die sich auf mehrere Konten auswirken können, und den allgemeinen Nutzungsbedingungen zuzustimmen.

Zum Abschluss

1. Überprüfen Sie an der Konsole die Serviceberechtigungen, und wenn Sie bereit sind, wählen Sie Ich verstehe die Berechtigungen, die AWS Control Tower für die Verwaltung von AWS Ressourcen und die Durchsetzung von Regeln in meinem Namen verwenden wird.
2. Um Ihre Auswahl zu treffen und den Start zu initialisieren, wählen Sie Landezone einrichten aus.

Mit dieser Reihe von Schritten wird der Prozess der Einrichtung deiner Landezone gestartet. Dieser Vorgang kann etwa dreißig Minuten in Anspruch nehmen. Während der Einrichtung erstellt AWS Control Tower Ihr Root-Level, die Sicherheits-OU und die gemeinsamen Konten. Andere AWS Ressourcen werden erstellt, geändert oder gelöscht.

⚠ Bestätigen Sie die SNS-Abonnements

Die E-Mail-Adresse, die Sie für das Auditkonto angegeben haben, erhält AWS Benachrichtigungen — Abonnementbestätigungs-E-Mails aus allen AWS Regionen, die von AWS Control Tower unterstützt werden. Um E-Mails zur Einhaltung der Vorschriften in Ihrem Auditkonto zu erhalten, müssen Sie in jeder E-Mail aus jeder AWS Region, die von AWS Control Tower unterstützt wird, auf den Link Abonnement bestätigen klicken.

Erste Schritte mit AWS Control Tower mithilfe von APIs

Dieses Verfahren für die ersten Schritte richtet sich an AWS Control Tower Tower-Administratoren. Dieses Verfahren erfordert einige Voraussetzungen und umfasst zwei Hauptschritte.

In diesem Verfahren verwenden Sie APIs von AWS Control Tower und anderen AWS Services, um eine landing zone zu konfigurieren und zu starten. Mit diesen APIs können Sie programmgesteuert eine AWS Control Tower Tower-Umgebung erstellen, entweder über die CloudFormation Konsole oder über die AWS CLI.

Bevor Sie Ihre AWS Control Tower Tower-Landezone starten, führen Sie die folgenden erforderlichen Aufgaben aus:

- Ermitteln Sie die am besten geeignete Heimatregion. Weitere Informationen finden Sie unter Administrative Tipps für die Einrichtung der landing zone.
- Lesen Sie Voraussetzung: Automatisierte Überprüfungen Ihres Verwaltungskontos vor dem Start weiter, um mehr über die automatisierten Prüfungen vor dem Start zu erfahren, mit denen sichergestellt wird, dass Ihr Verwaltungskonto für Änderungen bereit ist, mit denen Ihre landing zone eingerichtet wird.

Themen

- Erwartungen an die Konfiguration der landing zone mit APIs
- Schritt 1: Konfiguriere deine landing zone
- Schritt 2: Starten Sie Ihre landing zone mithilfe der AWS Control Tower Tower-APIs
- Identifizieren Sie Ihre landing zone
- Aktualisiere deine landing zone
- Setze die landing zone zurück, um Drift zu beheben

- Sehen Sie sich die Details Ihrer Landezonen-Manifestdatei an
- Sehen Sie sich den Status Ihrer Landezonenoperationen an
- Beispiele: Richten Sie eine AWS Control Tower-Landezone nur mit APIs ein
- Landezonenschemata
- Starte eine landing zone mit CloudFormation

Erwartungen an die Konfiguration der landing zone mit APIs

Die Einrichtung Ihrer AWS Control Tower Tower-Landezone landing zone aus mehreren Schritten. Bestimmte Aspekte Ihrer AWS Control Tower Tower-Landezone sind konfigurierbar. Andere Optionen können nach der Einrichtung nicht geändert werden.

Wichtige Elemente, die während der Einrichtung konfiguriert werden müssen

- Sie können Ihre Foundational OU-Namen während der Einrichtung auswählen und Sie können die OU-Namen auch ändern, nachdem Sie Ihre landing zone eingerichtet haben. Standardmäßig heißen die Foundation-Organisationseinheiten Security und Sandbox. Weitere Informationen finden Sie unter Richtlinien für die Einrichtung einer gut strukturierten Umgebung.
- Während der Einrichtung können Sie benutzerdefinierte Namen für die gemeinsamen Konten auswählen, die AWS Control Tower erstellt. Diese Namen werden standardmäßig als Log Archive und Audit bezeichnet, aber Sie können diese Namen nach der Einrichtung nicht mehr ändern. (Dies ist eine einmalige Auswahl.)
- Während der Einrichtung mit APIs müssen Sie bestehende AWS Konten angeben, die AWS Control Tower als Audit- und Protokollarchivkonten verwenden soll. Um bestehende AWS Konten anzugeben, müssen Sie, falls diese Konten über vorhandene AWS Config Ressourcen verfügen, die vorhandenen AWS Config Ressourcen löschen oder ändern, bevor Sie die Konten bei AWS Control Tower registrieren können. (Dies ist eine einmalige Auswahl.)
- Wenn Sie das System zum ersten Mal einrichten oder ein Upgrade auf landing zone Version 3.0 durchführen, können Sie wählen, ob Sie AWS Control Tower erlauben möchten, einen AWS CloudTrail Trail auf Organisationsebene für Ihr Unternehmen einzurichten, oder Sie können sich von Trails abmelden, die von AWS Control Tower verwaltet werden, und Ihre eigenen CloudTrail Trails verwalten. Sie können Trails auf Organisationsebene, die von AWS Control Tower verwaltet werden, jederzeit aktivieren oder deaktivieren, wenn Sie Ihre landing zone aktualisieren.

- Sie können optional eine benutzerdefinierte Aufbewahrungsrichtlinie für Ihren Amazon S3 S3-Log-Bucket und Ihren Log-Zugriffs-Bucket festlegen, wenn Sie Ihre landing zone einrichten oder aktualisieren.

Konfigurationsoptionen, die nicht rückgängig gemacht werden können

- Du kannst deine Heimatregion nicht ändern, nachdem du deine landing zone eingerichtet hast.
- Wenn Sie Konten mit VPCs bereitstellen, können VPC-CIDRs nach ihrer Erstellung nicht mehr geändert werden.

In den nächsten Abschnitten werden die Voraussetzungen und Schritte für die Einrichtung detailliert beschrieben, mit Erläuterungen und Einschränkungen. Weitere Codebeispiele finden Sie unterBeispiele: Richten Sie eine AWS Control Tower-Landezone nur mit APIs ein.

Schritt 1: Konfiguriere deine landing zone

Die Einrichtung Ihrer AWS Control Tower Tower-Landezone landing zone aus mehreren Schritten. Bestimmte Aspekte Ihrer AWS Control Tower Tower-Landezone sind konfigurierbar, andere Optionen können jedoch nach der Einrichtung nicht geändert werden. Weitere Informationen zu diesen wichtigen Überlegungen vor dem Start Ihrer landing zone finden Sie unter Erwartungen an die Konfiguration der landing zone.

Bevor Sie die AWS Control Tower landing zone Zone-APIs verwenden können, müssen Sie zunächst APIs von anderen AWS Services aufrufen, um Ihre landing zone vor dem Start zu konfigurieren. Der Prozess umfasst drei Hauptschritte:

1. Gründung einer neuen AWS Organisationsorganisation,
2. Einrichtung Ihrer Serviceintegrationskonten,
3. und eine IAM-Rolle oder einen IAM Identity Center-Benutzer mit den erforderlichen Berechtigungen zum Aufrufen der Landingzone-APIs zu erstellen.

Schritt 1. Erstellen Sie die Organisation, die Ihre landing zone enthalten soll:

Rufen Sie die AWS Organizations `CreateOrganization` API auf und aktivieren Sie alle Funktionen, um die Foundational OU zu erstellen. AWS Control Tower empfiehlt außerdem, eine spezielle Sicherheits-OU zu erstellen. Diese Sicherheits-OU sollte alle Ihre Service-

Integrationskonten enthalten. Dies wären das Protokollarchivkonto und das Auditkonto für frühere Landing Zone-Versionen.

```
aws organizations create-organization --feature-set ALL
```

AWS Control Tower kann eine oder mehrere zusätzliche Organisationseinheiten einrichten. Wir empfehlen Ihnen, neben der Sicherheits-OU mindestens eine zusätzliche Organisationseinheit in Ihrer landing zone bereitzustellen. Wenn diese zusätzliche Organisationseinheit für Entwicklungsprojekte vorgesehen ist, empfehlen wir Ihnen, sie Sandbox-Organisationseinheit zu nennen, wie es in der AWS-Strategie für mehrere Konten für Ihre AWS Control Tower-Landing landing zone angegeben ist.

Schritt 2. Stellen Sie bei Bedarf Konten für die Serviceintegration bereit:

Um Ihre landing zone einzurichten, ermöglicht AWS Control Tower Kunden die Konfiguration von AWS-Serviceintegrationen. Für jede dieser Serviceintegrationen sind möglicherweise ein oder mehrere zentrale Konten für die Serviceintegration erforderlich. Wenn Sie landing zone Zone-APIs verwenden, um AWS Control Tower zum ersten Mal einzurichten, müssen Sie das zentrale Integrationskonto für jede aktivierte AWS-Serviceintegration angeben. Sie können bestehende AWS-Konten verwenden oder diese Konten über die AWS Control Tower-Konsole oder die AWS Organisations-APIs bereitstellen. Stellen Sie sicher, dass sich diese Serviceintegrationskonten in der angegebenen Sicherheits-OU befinden, die sich auf der Stammebene in Ihrer Organisation befindet.

1. Rufen Sie die AWS Organizations `CreateAccount` API auf, um das Protokollarchiv-Konto und das Audit-Konto in der Sicherheits-OU zu erstellen.

   ```
   aws organizations create-account --email mylog@example.com --account-name "Logging
    Account"
   aws organizations create-account --email mysecurity@example.com --account-name
    "Security Account"
   ```

   (Optional) Überprüfen Sie den Status des `CreateAccount` Vorgangs mithilfe der AWS Organizations `DescribeAccount` API.

2. Verschieben Sie die bereitgestellten Serviceintegrationskonten in die angegebene Sicherheits-OU

   ```
   aws organizations move-account \
       --account-id 0123456789012 \
       --source-parent-id r-examplerootid111 \
   ```

```
    --destination-parent-id ou-examplerootid111-security
```

Schritt 3. Erstellen Sie die erforderlichen Servicerollen

Erstellen Sie die folgenden IAM-Servicerollen im `/service-role/` IAM-Pfad, die es AWS Control Tower ermöglichen, die API-Aufrufe durchzuführen, die für die Einrichtung Ihrer landing zone erforderlich sind:

- `AWSControlTowerAdmin`
- `AWSControlTowerCloudTrailRole`
- `AWSControlTowerStackSetRole`
- `AWSControlTowerConfigAggregatorRoleForOrganizations`(nicht erforderlich für landing zone Version 4.0 und höher)

Weitere Informationen zu diesen Rollen und ihren Richtlinien finden Sie unterVerwenden identitätsbasierter Richtlinien (IAM-Richtlinien) für AWS Control Tower.

So erstellen Sie eine IAM-Rolle:

Erstellen Sie eine IAM-Rolle mit den erforderlichen Berechtigungen, um alle Landingzone-APIs aufzurufen. Alternativ können Sie einen IAM Identity Center-Benutzer erstellen und ihm die erforderlichen Berechtigungen zuweisen.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "backup:UpdateGlobalSettings",
                "controltower:CreateLandingZone",
                "controltower:UpdateLandingZone",
                "controltower:ResetLandingZone",
                "controltower:DeleteLandingZone",
                "controltower:GetLandingZoneOperation",
                "controltower:GetLandingZone",
                "controltower:ListLandingZones",
                "controltower:ListLandingZoneOperations",
```

```
                "controltower:ListTagsForResource",
                "controltower:TagResource",
                "controltower:UntagResource",
                "servicecatalog:*",
                "organizations:*",
                "organizations:RegisterDelegatedAdministrator",
                "organizations:EnableAWSServiceAccess",
                "organizations:DeregisterDelegatedAdministrator",
                "organizations:ListDelegatedAdministrators",
                "sso:*",
                "sso-directory:*",
                "logs:*",
                "cloudformation:*",
                "kms:*",
                "iam:GetRole",
                "iam:CreateRole",
                "iam:GetSAMLProvider",
                "iam:CreateSAMLProvider",
                "iam:CreateServiceLinkedRole",
                "iam:ListRolePolicies",
                "iam:PutRolePolicy",
                "iam:ListAttachedRolePolicies",
                "iam:AttachRolePolicy",
                "iam:DeleteRole",
                "iam:DeleteRolePolicy",
                "iam:DetachRolePolicy"
            ],
            "Resource": "*"
        }
    ]
}
```

> **Note**
>
> Beim Upgrade auf landing zone Version 4.0 mit aktivierter AWS Config-Integration benötigen Kunden `organizations:ListDelegatedAdministrators` Berechtigungen.

Schritt 2: Starten Sie Ihre landing zone mithilfe der AWS Control Tower Tower-APIs

Sie können die AWS Control Tower Tower-APIs verwenden, um Ihre landing zone zu starten. In diesem Abschnitt wird beschrieben, wie Sie die erforderliche Landingzone-Manifestdatei erstellen und sie mit dem `CreateLandingZone` API-Vorgang verwenden.

Die Manifestdatei wird erstellt

Die Manifestdatei ist ein JSON-Dokument, das Ihre Landezonenkonfiguration spezifiziert. Mit landing zone Version 4.0 sind viele Komponenten jetzt optional, was einen flexibleren Einsatz ermöglicht.

Manifeste Struktur

Im Folgenden finden Sie die vollständige Struktur der Manifestdatei mit allen verfügbaren Konfigurationen:

```
{
    "accessManagement": {
        "enabled": true    // Required - Controls IAM Identity Center integration
    },
    "backup": {
        "enabled": true,   // Required - Controls AWS Backup integration
        "configurations": {
            "backupAdmin": {
                "accountId": "111122223333"    // Backup administrator account
            },
            "centralBackup": {
                "accountId": "111122224444"    // Central backup account
            },
            "kmsKeyArn": "arn:aws:kms:region:account-id:key/key-id"
        }
    },
    "centralizedLogging": {
        "accountId": "111122225555",    // Log archive account
        "enabled": true,                // Required - Controls centralized logging
        "configurations": {
            "accessLoggingBucket": {
                "retentionDays": 365    // Minimum value: 1
            },
            "loggingBucket": {
```

```
                "retentionDays": 365    // Minimum value: 1
            },
            "kmsKeyArn": "arn:aws:kms:region:account-id:key/key-id"
        }
    },
    "config": {
        "accountId": "111122226666",    // Config aggregator account
        "enabled": true,                // Required - Controls AWS Config integration
        "configurations": {
            "accessLoggingBucket": {
                "retentionDays": 365    // Minimum value: 1
            },
            "loggingBucket": {
                "retentionDays": 365    // Minimum value: 1
            },
            "kmsKeyArn": "arn:aws:kms:region:account-id:key/key-id"
        }
    },
    "governedRegions": [              // Optional - List of regions to govern
        "us-east-1",
        "us-west-2"
    ],
    "securityRoles": {
        "enabled": true,              // Required - Controls security roles creation
        "accountId": ""111122226666"    // Security/Audit account
    }
}
```

Wichtige Hinweise

- Alle `enabled` Flags sind im Manifest erforderlich.
- Wenn Sie die AWS Config-Integration (`"config.enabled": false`) deaktivieren, müssen Sie auch die folgenden Integrationen deaktivieren:
  - Sicherheitsrollen () `"securityRoles.enabled": false`
  - Zugriffsverwaltung (`"accessManagement.enabled": false`)
  - Backup (`"backup.enabled": false`)
- Konto-IDs müssen gültige 12-stellige AWS Konto-IDs sein.
- KMS-Schlüssel-ARNs müssen gültige AWS KMS Schlüssel-ARNs sein.
- Die Aufbewahrungszeit muss mindestens 1 Tage betragen.

Verwenden der CreateLandingZone API

So erstellen Sie Ihre landing zone mithilfe der API:

```
aws controltower create-landing-zone --landing-zone-version 4.0 --manifest file://
manifest.json
```

Die API gibt eine Betriebs-ID für die landing zone zurück, mit der Sie den Fortschritt der Erstellung Ihrer landing zone verfolgen können. Beispielantwort:

```
{
    "arn": "arn:aws:controltower:us-west-2:123456789012:landingzone/1A2B3C4D5E6F7G8H",
    "operationIdentifier": "55XXXXXX-e2XX-41XX-a7XX-446XXXXXXXXX"
}
```

Sie können den Betriebsstatus mithilfe der `GetLandingZoneOperation` API überwachen, die einen Status von `SUCCEEDEDFAILED`, oder zurückgibt`IN_PROGRESS`:

```
aws controltower get-landing-zone-operation --operation-identifier "55XXXXXX-eXXX-4XXX-
aXXX-44XXXXXXXXXX"
```

Was hat sich in landing zone Version 4.0 geändert

Wichtige Änderungen an der Manifeststruktur und den Anforderungen:

- Struktur der Organisation
  - `organizationStructure`Die Definition wurde aus dem Manifest entfernt
  - Kunden können jetzt ihre eigene Organisationsstruktur definieren
  - Einzige Voraussetzung: Serviceintegrationskonten müssen sich in derselben Organisationseinheit direkt unter Root befinden
- Flags aktiviert
  - Alle Konfigurationen der Serviceintegration haben ein `enabled` Flag, das jetzt ein Pflichtfeld ist.
  - Kunden müssen immer einen booleschen Wert angeben. Es werden keine Standardwerte angegeben.
  - Kunden müssen enable/disable jede Serviceintegrationskonfiguration im Manifest explizit angeben:

    - `accessManagement`
    - `backup`
    - `centralizedLogging`
    - `config`
    - `securityRoles`
- Sicherheitsrollen
  - Die Integration von Sicherheitsrollen ist jetzt optional
  - Es wurde eine neue `enabled` Flagge zur Verwaltung der `securityRoles` Bereitstellung eingeführt
  - Wenn diese Option deaktiviert ist, werden die entsprechenden Sicherheitsfunktionen nicht implementiert
- AWS Config
  - Dem Manifest wurde ein neuer Abschnitt zur AWS-Config-Serviceintegration hinzugefügt, der die folgenden Felder enthält: `config`
    - `enabled`: Boolesches Flag erforderlich, um die Bereitstellung der AWS Config-Integration zu verwalten
    - `accountId`: AWS-Konto-ID für den AWS Config-Aggregator
    - Konfigurationen:
      - `accessLoggingBucket.retentionDays`: Aufbewahrungsfrist für Zugriffsprotokolle
      - `loggingBucket.retentionDays`: Aufbewahrungszeitraum für AWS Config-Protokolle
      - `kmsKeyArn`: KMS-Schlüssel für die Verschlüsselung

Identifizieren Sie Ihre landing zone

Wenn Sie anrufen, `ListLandingZones` können Sie feststellen, ob Ihr Konto bereits bei AWS Control Tower eingerichtet ist. Diese API gibt eine Landing Zone Identifier (ARN) für jede kommerzielle Region zurück, unabhängig von der Heimatregion der landing zone. Landezone-ARNs sind regional einzigartig.

```
aws controltower list-landing-zones --region us-east-1
```

Für Opt-in-Regionen gibt die `ListLandingZones` API die landing zone Identifier nur zurück, wenn Sie die API in derselben Region aufrufen wie die Heimatregion der API. Wenn Ihre landing zone

beispielsweise in af-south-1 eingerichtet ist und Sie af-south-1 aufrufen`ListLandingZones`, gibt die API die Landezonen-ID zurück. Wenn Ihre landing zone in af-south-1 eingerichtet ist und Sie ap-east-1 aufrufen`ListLandingZones`, gibt die API die Landezonen-ID nicht zurück.

Ausgabe:

```
{
   "landingZones" [
        "arn": "arn:aws:controltower:us-
west-2:123456789123:landingzone/1A2B3C4D5E6F7G8H"
   ]
}
```

Aktualisiere deine landing zone

Wenn eine neue Landingzone-Version verfügbar ist oder um andere Aktualisierungen an Ihrer Landingzone-Konfiguration vorzunehmen, können Sie die `UpdateLandingZone` API aufrufen und auf eine aktualisierte Landingzone-Manifestdatei verweisen. Diese API gibt eine zurück`OperationIdentifier`, die Sie dann verwenden können, wenn Sie die `GetLandingZoneOperation` API aufrufen, um den Status des Aktualisierungsvorgangs zu überprüfen.

Um die landing zone zu aktualisieren

1. Rufen Sie die AWS Control Tower `UpdateLandingZone` API auf und verweisen Sie auf die aktualisierte landing zone Zone-Version oder Ihre aktualisierte landing zone Zone-Manifestdatei.

   ```
   aws controltower update-landing-zone --landing-zone-version 3.3 --landing-zone-
   identifier "arn:aws:controltower:us-west-2:123456789123:landingzone/1A2B3C4D5E6F7G8H"
    --manifest file://LandingZoneManifest.json
   ```

LandingZoneManifest.jsonBeispieldatei mit Regionen und zentraler Protokollierung:

```
{
   "governedRegions": ["us-west-2","us-west-1"],
   "organizationStructure": {
       "security": {
           "name": "Security"
       },
```

```
        "sandbox": {
            "name": "Sandbox"
        }
    },
    "centralizedLogging": {
         "accountId": "LOG ARCHIVE ACCOUNT ID",
         "configurations": {
             "loggingBucket": {
                 "retentionDays":2555
             },
             "accessLoggingBucket": {
                 "retentionDays": 2555
             },
             "kmsKeyArn": "arn:aws:kms:us-west-1:123456789123:key/
e84XXXXX-6bXX-49XX-9eXX-ecfXXXXXXXXX"
         },
         "enabled": true
    },
    "securityRoles": {
         "accountId": "SECURITY ACCOUNT ID"
    },
    "accessManagement": {
         "enabled": true
    }
}
```

Ausgabe:

```
{
   "operationIdentifier": "55XXXXXX-e2XX-41XX-a7XX-446XXXXXXXXX"
}
```

> **Optionale Re-register OU zur Aktualisierung von Konten**
>
> Für registrierte AWS Control Tower Tower-Organisationseinheiten mit weniger als 1000 Konten können Sie die AWS Control Tower Tower-Konsole verwenden, auf die OU-Seite im Dashboard zugreifen und Re-registerOU auswählen, um die Konten in dieser OU zu aktualisieren.

Setze die landing zone zurück, um Drift zu beheben

Wenn Sie Ihre landing zone erstellen, entsprechen die landing zone und alle Organisationseinheiten (OUs), Konten und Ressourcen den Governance-Regeln, die durch die von Ihnen ausgewählten Kontrollen durchgesetzt werden. Wenn Sie und Ihre Organisationsmitglieder die landing zone nutzen, kann es zu Änderungen dieses Compliance-Status kommen. Diese Änderungen werden als Drift bezeichnet.

Um festzustellen, ob sich Ihre landing zone in Drift befindet, können Sie die `GetLandingZone` API aufrufen. Diese API gibt den Drift-Status der Landezone von `DRIFTED` oder zurück`IN_SYNC`.

Um Abweichungen innerhalb Ihrer landing zone zu beheben, können Sie die `ResetLandingZone` API verwenden, um die landing zone auf ihre ursprüngliche Konfiguration zurückzusetzen. Zum Beispiel aktiviert AWS Control Tower standardmäßig IAM Identity Center, um Sie bei der Verwaltung Ihrer Daten zu unterstützen. Wenn Sie Ihre AWS-Konten ursprünglichen Landingzone-Parameter jedoch so konfigurieren, dass IAM Identity Center deaktiviert ist, wird beim Aufrufen die deaktivierte IAM Identity Center-Konfiguration `ResetLandingZone` beibehalten.

Sie können die `ResetLandingZone` API nur verwenden, wenn Ihre landing zone Version 3.1 oder höher hat. Sie können die `GetLandingZone` API aufrufen, um Ihre aktuelle landing zone Zone-Version zu überprüfen. Wenn sich Ihre landing zone auf einer Version vor 3.1 befindet, ist die `ResetLandingZone` API nicht verfügbar. In diesem Fall Aktualisiere deine landing zone mindestens Version 3.1. Der Aktualisierungsvorgang behebt die Drift von selbst, sodass Sie das Gerät nicht separat zurücksetzen müssen. Durch das Zurücksetzen Ihrer landing zone wird sie nicht auf die neueste verfügbare Version aktualisiert.

1. Rufen Sie die `GetLandingZone`-API auf. Wenn die API den Drift-Status von zurückgibt`DRIFTED`, befindet sich Ihre landing zone im Drift-Modus.
2. Rufen Sie die `ResetLandingZone` API auf, um Ihre landing zone auf die ursprüngliche Konfiguration zurückzusetzen.

```
aws controltower reset-landing-zone --landing-zone-identifier
 "arn:aws:controltower:us-west-2:123456789123:landingzone/1A2B3C4D5E6F7G8H"
```

Ausgabe:

```
{
   "operationIdentifier": "55XXXXXX-e2XX-41XX-a7XX-446XXXXXXXXX"
```

```
}
```

> **Note**
>
> Durch das Zurücksetzen der landing zone wird die Landezonenversion nicht aktualisiert. Einzelheiten Aktualisiere deine landing zone zur Aktualisierung der landing zone Zone-Version finden Sie hier.

Sehen Sie sich die Details Ihrer Landezonen-Manifestdatei an

Die Manifestdatei der AWS Control Tower Landing Zone ist eine Textdatei, die Ihre AWS Control Tower-Ressourcen beschreibt. Die folgenden Abschnitte enthalten detaillierte Definitionen der Einträge in der Landing Zone-Manifestdatei.

Ein vollständiges Beispiel für ein Landezonenschema finden Sie unter Landezonenschemas.

Regierte Regionen — Regionen, die der Verwaltung unterstellt werden sollen

- Typ: Auflistung von Zeichenfolgen
- Required: No
- Beispiel:

```
"governedRegions": ["us-west-2","us-west-1"]
```

OrganizationStructure — Wählen Sie die Namen der Sicherheits- und Sandbox-OUs aus, die in Ihrer Organisation erstellt werden sollen

- Typ: Objekt
- Erforderlich: Ja
- Eigenschaften:
- Beispiel:
  - `security`- ein Objekt mit einer erforderlichen Eigenschaft`name`, das eine `String`
  - `sandbox`- ein Objekt mit einer erforderlichen Eigenschaft`name`, das eine `String`

```
"organizationStructure": {
      "security": {
```

```
            "name": "CORE"
        },
        "sandbox": {
            "name": "Sandbox"
        }
    }
```

> **Note**
>
> Das `organizationStructure` Feld ist in der Landing Zone-Version 4.0 und höher nicht vorhanden.

CentralizedLogging — Konfiguration für AWS CloudTrail

- Typ: Objekt
- Erforderlich: Nein (Version 4.0 und höher). Ja (Version 3.3 und früher).
- Eigenschaften:
  - accountID — a steht für `String` das AWS Konto, für das die Protokollierungsressource bereitgestellt werden soll
  - Konfigurationen — und `Object` mit drei Eigenschaften
    - `loggingBucket`- ein Objekt mit einer Eigenschaft`retentionDays`, das eine `Number`
    - `accessLoggingBucket`- ein Objekt mit einer Eigenschaft`retentionDays`, das eine `Number`
    - `kmsKeyArn`- ein optionales `String`
  - aktiviert — a `Boolean` (erforderlich in Version 4.0 und höher, optional in Version 3.3 und früher)
- Beispiel:

```
"centralizedLogging": {
        "accountId": "222222222222",
        "configurations": {
            "loggingBucket": {
                "retentionDays": 60
            },
            "accessLoggingBucket": {
                "retentionDays": 60
            },
```

```
            "kmsKeyArn": "arn:aws:kms:us-west-1:123456789123:key/
e84XXXXX-6bXX-49XX-9eXX-ecfXXXXXXXXX"
        },
        "enabled": true
   }
```

> **Note**
>
> In der Landing Zone-Version 4.0 und höher `accountId` ist dies nur erforderlich, wenn auf eingestellt `enabled` ist`true`. Das Feld `enabled` ist ein Pflichtfeld.

SecurityRoles — Wählen Sie aus, wo zentrale Ressourcen für die Sicherheitsüberwachung in Ihrem Unternehmen eingesetzt werden sollen

- Typ: Objekt
- Erforderlich: Nein (Version 4.0 und höher). Ja (Version 3.3 und früher).
- Eigenschaften:
  - AccountID — eine`String`, die das AWS Konto darstellt, für das die zentralen Ressourcen zur Sicherheitsüberwachung bereitgestellt werden sollen. Erforderlich, wenn es `enabled` ist`true`.
  - aktiviert — a `Boolean` (erforderlich in Version 4.0 und höher)
- Beispiel:

```
"securityRoles": {
        "accountId": "333333333333",
        "enabled": true
   }
```

> **Note**
>
> `securityRoles`Enthält in der Landing Zone-Version 4.0 und höher eine erforderliche `enabled` boolesche Eigenschaft. Die `accountId` ist nur erforderlich, wenn auf gesetzt `enabled` ist. `true`

AccessManagement — Wählen Sie aus, ob die Zugriffsverwaltung aktiviert werden soll

- Typ: Objekt
- Required: No
- Eigenschaften: aktiviert — ein boolescher Wert
- Beispiel:

```
"accessManagement": {
        "enabled": true
   }
```

Backup — Konfiguration für die AWS Sicherung mit AWS Control Tower

- Typ: Objekt
- Required: No
- Eigenschaften:
  - Konfigurationen - eine `Object` mit drei Eigenschaften
    - `centralBackup`- ein Objekt mit einer Eigenschaft`accountId`, das eine `String`
    - `backupAdmin`- ein Objekt mit einer Eigenschaft`accountId`, das eine `String`
    - `kmsKeyArn`- ein optionales `String`
  - aktiviert - ein `Boolean`
- Beispiel:

```
"backup": {
    "configurations": {
        "centralBackup": {
            "accountId": "CENTRAL BACKUP ACCOUNT ID"
        },
        "backupAdmin": {
            "accountId": "BACKUP MANAGER ACCOUNT ID"
        },
        "kmsKeyArn": "arn:aws:kms:us-west-1:123456789123:key/e84XXXXX-6bXX-49XX-9eXX-
ecfXXXXXXXXX"
    },
    "enabled": true
}
```

config — Konfiguration für AWS Config mit AWS Control Tower

- Typ: Objekt
- Required: No
- Eigenschaften:
  - accountID — eine`String`, die das AWS Konto darstellt, für das die AWS Config Ressourcen bereitgestellt werden sollen. Erforderlich, wenn es `enabled` ist`true`.
  - Konfigurationen — eine optionale Konfiguration `Object` mit drei Eigenschaften
    - `loggingBucket`- ein Objekt mit einer Eigenschaft`retentionDays`, das eine `Number`
    - `accessLoggingBucket`- ein Objekt mit einer Eigenschaft`retentionDays`, das eine `Number`
    - `kmsKeyArn`- ein optionales `String`
  - aktiviert — ein erforderliches `Boolean`
- Beispiel:

```
"config": {
    "accountId": "444444444444",
    "configurations": {
        "loggingBucket": {
            "retentionDays": 60
        },
        "accessLoggingBucket": {
            "retentionDays": 60
        },
        "kmsKeyArn": "arn:aws:kms:us-west-1:123456789123:key/e84XXXXX-6bXX-49XX-9eXX-
ecfXXXXXXXXX"
    },
    "enabled": true
}
```

> **Note**
>
> Das `config` Feld ist nur in der Landing Zone-Version 4.0 und höher verfügbar.

Sehen Sie sich den Status Ihrer Landezonenoperationen an

Die `ListLandingZoneOperations` API ermöglicht es Ihnen, den Status der AWS Control Tower-Operationen einzusehen, die Aktionen in Ihrer Landezone ausführen.

Weitere Informationen zu diesem API-Vorgang finden Sie unter ListLandingZoneOperations.

ListLandingZoneOperations

Beispiel für Eingabe und Ausgabe für **`ListLandingZoneOperations`**.

Dieses Beispiel zeigt, wie die API ohne Parameter aufgerufen wird.

```
aws controltower --region us-east-1 list-landing-zone-operations

{
    "landingZoneOperations": [
        {
            "operationIdentifier": "873fe98d-1ecc-4154-b593-86e4a95ebfXX",
            "operationType": "CREATE",
            "status": "FAILED"
        },
        {
            "operationIdentifier": "0016d43d-a307-4ad8-a2a2-b427b8eb1cXX",
            "operationType": "DELETE",
            "status": "SUCCEEDED"
        },
        {
            "operationIdentifier": "002b8b5a-6bb7-4c40-89cd-5822a73d13XX",
            "operationType": "CREATE",
            "status": "SUCCEEDED"
        },
        {
            "operationIdentifier": "008886a0-f7a2-4df3-90e8-6e9f936507XX",
            "operationType": "CREATE",
            "status": "FAILED"
        }
    ]
}
```

Dieses Beispiel zeigt, wie die API aufgerufen und die maximale Anzahl von Ergebnissen angegeben wird.

```
aws controltower --region us-east-1 list-landing-zone-operations --max-results 1

{
    "landingZoneOperations": [
        {
            "operationIdentifier": "873fe98d-1ecc-4154-b593-86e4a95ebfXX",
            "operationType": "CREATE",
            "status": "FAILED"
        }
    ],
    "nextToken": "AAMAATFMzwP0QysYY8npWgstfcHGQBj-
XCC18ISyd9mkQmzLR7ZFMket4F0aWv8tUTtnsTWOnfblUp_Q9U-
nX9_6lEsLHs0RlhceDKskHr0_3fm8KdPTa6ofxMt5SPw8WF7-Jsvw2rJVvhj4DHDipo-y1HVK_eZ__Z3-
OzInm403cIHxhbjGPgqCX6FeKr8lwgTDKOejkLYZ9w7J5aqPAKLfVP8KKNda5g0VfMj1wdl4J2nwnHI-
UuCTIZ5nUEgXgUHaFq6Ma1pLDfGefZQJn5HmDhhgd5yvqzSRH1BtrHpdV_N1EVP8u3JJr3eWQHe9jNB02lihD4Mdcbm3SJg
VXRwTUIBInrit4HslNtPE8-IC1gxCjGoYPGtuWBPumK-pUPE="
}
```

Dieses Beispiel zeigt, wie Sie die API aufrufen und ein paginiertes Ergebnis mit `nextToken` erhalten.

```
aws controltower --region us-east-1 list-landing-zone-operations --next-token
 AAMAATFMzwP0QysYY8npWgstfcHGQBj-XCC18ISyd9mkQmzLR7ZFMket4F0aWv8tUTtnsTWOnfblUp_Q9U-
nX9_6lEsLHs0RlhceDKskHr0_3fm8KdPTa6ofxMt5SPw8WF7-Jsvw2rJVvhj4DHDipo-y1HVK_eZ__Z3-
OzInm403cIHxhbjGPgqCX6FeKr8lwgTDKOejkLYZ9w7J5aqPAKLfVP8KKNda5g0VfMj1wdl4J2nwnHI-
UuCTIZ5nUEgXgUHaFq6Ma1pLDfGefZQJn5HmDhhgd5yvqzSRH1BtrHpdV_N1EVP8u3JJr3eWQHe9jNB02lihD4Mdcbm3SJg
VXRwTUIBInrit4HslNtPE8-IC1gxCjGoYPGtuWBPumK-pUPE=

{
    "landingZoneOperations": [
        {
            "operationIdentifier": "0016d43d-a307-4ad8-a2a2-b427b8eb1cXX",
            "operationType": "DELETE",
            "status": "SUCCEEDED"
        },
        {
            "operationIdentifier": "002b8b5a-6bb7-4c40-89cd-5822a73d13XX",
            "operationType": "CREATE",
            "status": "SUCCEEDED"
        },
        {
            "operationIdentifier": "008886a0-f7a2-4df3-90e8-6e9f936507XX",
            "operationType": "CREATE",
            "status": "FAILED"
```

```
        }
    ]
}
```

Dieses Beispiel zeigt, wie die API mit einem Filter aufgerufen wird.

```
aws controltower --region us-east-1 list-landing-zone-operations --filter '{"types":
["CREATE"],"statuses":["FAILED"]}'

{
    "landingZoneOperations": [
        {
            "operationIdentifier": "873fe98d-1ecc-4154-b593-86e4a95ebfXX",
            "operationType": "CREATE",
            "status": "FAILED"
        },
        {
            "operationIdentifier": "008886a0-f7a2-4df3-90e8-6e9f936507XX",
            "operationType": "CREATE",
            "status": "FAILED"
        }
    ]
}
```

Beispiele: Richten Sie eine AWS Control Tower-Landezone nur mit APIs ein

Diese exemplarische Vorgehensweise mit Beispielen ist ein Begleitdokument. Erläuterungen, Vorbehalte und weitere Informationen finden Sie unter Erste Schritte mit AWS Control Tower mithilfe von APIs.

Voraussetzungen

Bevor Sie eine AWS Control Tower-Landing Zone erstellen, müssen Sie eine Organisation, zwei gemeinsame Konten und einige IAM-Rollen erstellen. Dieses Walkthrough-Tutorial beinhaltet die folgenden Schritte mit Beispielen für CLI-Befehle und -Ausgaben.

Schritt 1. Erstellen Sie die Organisation und zwei erforderliche Konten.

```
aws organizations create-organization --feature-set ALL
aws organizations create-account --email example+log@example.com --account-name "Log
 archive account"
```

```
aws organizations create-account --email example+aud@example.com --account-name "Audit
 account"
```

Schritt 2. Erstellen Sie die erforderlichen IAM-Rollen.

AWSControlTowerAdmin

```
cat <<EOF >controltower_trust.json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "controltower.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
EOF
aws iam create-role --role-name AWSControlTowerAdmin --path /service-role/ --assume-
role-policy-document file://controltower_trust.json
cat <<EOF >ct_admin_role_policy.json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:DescribeAvailabilityZones",
            "Resource": "*"
        }
    ]
}
EOF
aws iam put-role-policy --role-name AWSControlTowerAdmin --policy-name
 AWSControlTowerAdminPolicy --policy-document file://ct_admin_role_policy.json
aws iam attach-role-policy --role-name AWSControlTowerAdmin --policy-arn
 arn:aws:iam::aws:policy/service-role/AWSControlTowerServiceRolePolicy
```

AWSControlTowerCloudTrailRole

```
cat <<EOF >cloudtrail_trust.json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudtrail.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
EOF
aws iam create-role --role-name AWSControlTowerCloudTrailRole --path /service-role/ --
assume-role-policy-document file://cloudtrail_trust.json
cat <<EOF >cloudtrail_role_policy.json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": "logs:CreateLogStream",
            "Resource": "arn:aws:logs:*:*:log-group:aws-controltower/CloudTrailLogs:*",
            "Effect": "Allow"
        },
        {
            "Action": "logs:PutLogEvents",
            "Resource": "arn:aws:logs:*:*:log-group:aws-controltower/CloudTrailLogs:*",
            "Effect": "Allow"
        }
    ]
}
EOF
aws iam put-role-policy --role-name AWSControlTowerCloudTrailRole --
policy-name AWSControlTowerCloudTrailRolePolicy --policy-document file://
cloudtrail_role_policy.json
```

AWSControlTowerStackSetRole

```
cat <<EOF >cloudformation_trust.json
{
    "Version": "2012-10-17",
    "Statement": [
```

```
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudformation.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
EOF
aws iam create-role --role-name AWSControlTowerStackSetRole --path /service-role/ --
assume-role-policy-document file://cloudformation_trust.json
cat <<EOF >stackset_role_policy.json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "sts:AssumeRole"
            ],
            "Resource": [
                "arn:aws:iam::*:role/AWSControlTowerExecution"
            ],
            "Effect": "Allow"
        }
    ]
}
EOF
aws iam put-role-policy --role-name AWSControlTowerStackSetRole --policy-name
 AWSControlTowerStackSetRolePolicy --policy-document file://stackset_role_policy.json
```

AWSControlTowerConfigAggregatorRoleForOrganizations

```
cat <<EOF >config_trust.json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "config.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
```

```
        }
    ]
}
EOF
aws iam create-role --role-name AWSControlTowerConfigAggregatorRoleForOrganizations --
path /service-role/ --assume-role-policy-document file://config_trust.json
aws iam attach-role-policy --role-name
 AWSControlTowerConfigAggregatorRoleForOrganizations --policy-arn
 arn:aws:iam::aws:policy/service-role/AWSConfigRoleForOrganizations
```

Schritt 3. Rufen Sie Konto-IDs ab und generieren Sie die Landezone-Manifestdatei.

Die ersten beiden Befehle im folgenden Beispiel speichern die Konto-IDs für die Konten, die Sie in Schritt 1 erstellt haben, in Variablen. Diese Variablen helfen dann bei der Generierung der Landing Zone-Manifestdatei.

```
sec_account_id=$(aws organizations list-accounts | jq -r '.Accounts[] | select(.Name ==
 "Audit account") | .Id')
log_account_id=$(aws organizations list-accounts | jq -r '.Accounts[] | select(.Name ==
 "Log archive account") | .Id')

cat <<EOF >landing_zone_manifest.json
{
   "governedRegions": ["us-west-1", "us-west-2"],
   "organizationStructure": {
       "security": {
           "name": "Security"
       },
       "sandbox": {
           "name": "Sandbox"
       }
   },
   "centralizedLogging": {
        "accountId": "$log_account_id",
        "configurations": {
            "loggingBucket": {
                "retentionDays": 60
            },
            "accessLoggingBucket": {
                "retentionDays": 60
            }
        },
        "enabled": true
```

```
   },
   "securityRoles": {
        "accountId": "$sec_account_id"
   },
   "accessManagement": {
        "enabled": true
   }
}
EOF
```

Schritt 4. Erstellen Sie die Landezone mit der neuesten Version.

Sie müssen die Landezone mit der Manifestdatei und der neuesten Version einrichten. Dieses Beispiel zeigt Version 3.3.

```
aws --region us-west-1 controltower create-landing-zone --manifest file://
landing_zone_manifest.json --landing-zone-version 3.3
```

Die Ausgabe enthält einen ARN und einen OperationIdentifier, wie im folgenden Beispiel gezeigt.

```
{
    "arn": "arn:aws:controltower:us-west-1:0123456789012:landingzone/4B3H0ULNUOL2AXXX",
    "operationIdentifier": "16bb47f7-b7a2-4d90-bc71-7df4ca1201xx"
}
```

Schritt 5. (Optional) Verfolgen Sie den Status Ihrer Operation zur Erstellung der Landezone, indem Sie eine Schleife einrichten.

Um den Status zu verfolgen, verwenden Sie den OperationIdentifier aus der Ausgabe des vorherigen `create-landing-zone` Befehls.

```
aws --region us-west-1 controltower get-landing-zone-operation --operation-identifier
 16bb47f7-b7a2-4d90-bc71-7df4ca1201xx
```

Beispiel für eine Statusausgabe:

```
{
    "operationDetails": {
        "operationType": "CREATE",
        "startTime": "2024-02-28T21:49:31Z",
        "status": "IN_PROGRESS"
    }
```

```
}
```

Sie können das folgende Beispielskript verwenden, um eine Schleife einzurichten, die den Status des Vorgangs wie eine Protokolldatei immer wieder meldet. Dann müssen Sie den Befehl nicht immer wieder eingeben.

```
while true; do echo "$(date) $(aws --region us-west-1 controltower get-landing-
zone-operation --operation-identifier 16bb47f7-b7a2-4d90-bc71-7df4ca1201xx | jq -
r .operationDetails.status)"; sleep 15; done
```

Um detaillierte Informationen über Ihre Landezone anzuzeigen

Schritt 1. Ermitteln Sie den ARN der Landezone

```
aws --region us-west-1 controltower list-landing-zones
```

Die Ausgabe enthält die Kennung der Landezone, wie im folgenden Ausgabebeispiel gezeigt.

```
{
    "landingZones": [
        {
            "arn": "arn:aws:controltower:us-
west-1:123456789012:landingzone/4B3H0ULNUOL2AXXX"
        }
    ]
}
```

Schritt 2. Holen Sie sich die Informationen

```
aws --region us-west-1 controltower get-landing-zone --landing-zone-identifier
 arn:aws:controltower:us-west-1:123456789012:landingzone/4B3H0ULNUOL2AXXX
```

Hier ist ein Beispiel für die Art der Ausgabe, die Sie möglicherweise sehen:

```
{
    "landingZone": {
        "arn": "arn:aws:controltower:us-
west-1:123456789012:landingzone/4B3H0ULNUOL2AXXX",
        "driftStatus": {
            "status": "IN_SYNC"
        },
```

```
        "latestAvailableVersion": "3.3",
        "manifest": {
            "accessManagement": {
                "enabled": true
            },
            "securityRoles": {
                "accountId": "9750XXXX4444"
            },
            "governedRegions": [
                "us-west-1",
                "us-west-2"
            ],
            "organizationStructure": {
                "sandbox": {
                    "name": "Sandbox"
                },
                "security": {
                    "name": "Security"
                }
            },
            "centralizedLogging": {
                "accountId": "012345678901",
                "configurations": {
                    "loggingBucket": {
                        "retentionDays": 60
                    },
                    "accessLoggingBucket": {
                        "retentionDays": 60
                    }
                },
                "enabled": true
            }
        },
        "status": "ACTIVE",
        "version": "3.3"
    }
}
```

Schritt 6: (Optional) Rufen Sie die **`ListLandingZoneOperations`** API auf, um den Status aller Operationen einzusehen, die Ihre Landezone ändern.

Um den Status einer Landezonenoperation zu verfolgen, können Sie die ListLandingZoneOperations API aufrufen.

Landezonenschemata

Eine landing zone ist eine AWS Ressource, die mithilfe von Schemas erstellt wird. Jede Version der AWS Control Tower landing zone hat ein einzigartiges Schema.

Die Schemas für AWS Control Tower Tower-Landezonen, Version 3.1 und neuer, werden in diesem Referenzabschnitt veröffentlicht, um Ihnen bei der Auswahl einer kompatiblen Version zu helfen.

> **Note**
>
> Ein bekanntes Problem mit der Protokollierung unnötiger Zugriffe ist in landing zone Version 3.0 vorhanden. Das Problem wurde in landing zone Version 3.1 behoben. Weitere Informationen zu den Änderungen finden Sie unterAWS Control Tower-Landezone, Version 3.1.

Schema der Landezone 4.0

```
{
    "type": "object",
    "required": [],
    "properties": {
        "accessManagement": {
            "$ref": "#/definitions/AccessManagement"
        },
        "backup": {
            "$ref": "#/definitions/Backup"
        },
        "centralizedLogging": {
            "$ref": "#/definitions/CentralizedLogging"
        },
        "governedRegions": {
            "type": "array",
            "items": {
                "type": "string",
                "maxLength": 24,
                "minLength": 1,
                "pattern": "^[a-z]{2}-[a-z\\-]*-[0-9]{1}$",
                "additionalProperties": false
            },
            "additionalProperties": false
        },
```

```
        "securityRoles": {
            "$ref": "#/definitions/SecurityRoles"
        },
        "config": {
            "$ref": "#/definitions/Config"
        }
    },
    "additionalProperties": false,
    "definitions": {
        "AccessManagement": {
            "type": "object",
            "required": [
                "enabled"
            ],
            "properties": {
                "enabled": {
                    "type": "boolean",
                    "additionalProperties": false
                }
            },
            "additionalProperties": false
        },
        "Backup": {
            "type": "object",
            "required": [
                "enabled"
            ],
            "properties": {
                "configurations": {
                    "$ref": "#/definitions/BackupConfigurations"
                },
                "enabled": {
                    "type": "boolean",
                    "additionalProperties": false
                }
            },
            "additionalProperties": false,
            "if": {
                "properties": {
                    "enabled": {
                        "const": true
                    }
                }
            },
```

```
            "then": {
                "required": [
                    "configurations"
                ]
            }
        },
        "BackupAdminConfigurations": {
            "type": "object",
            "required": [
                "accountId"
            ],
            "properties": {
                "accountId": {
                    "type": "string",
                    "maxLength": 12,
                    "minLength": 12,
                    "pattern": "^\\d{12}$",
                    "additionalProperties": false
                }
            },
            "additionalProperties": false
        },
        "BackupConfigurations": {
            "type": "object",
            "required": [
                "backupAdmin",
                "centralBackup",
                "kmsKeyArn"
            ],
            "properties": {
                "backupAdmin": {
                    "$ref": "#/definitions/BackupAdminConfigurations"
                },
                "centralBackup": {
                    "$ref": "#/definitions/CentralBackupConfigurations"
                },
                "kmsKeyArn": {
                    "type": "string",
                    "maxLength": 2048,
                    "minLength": 1,
                    "additionalProperties": false
                }
            },
            "additionalProperties": false
```

```
        },
        "CentralBackupConfigurations": {
            "type": "object",
            "required": [
                "accountId"
            ],
            "properties": {
                "accountId": {
                    "type": "string",
                    "maxLength": 12,
                    "minLength": 12,
                    "pattern": "^\\d{12}$",
                    "additionalProperties": false
                }
            },
            "additionalProperties": false
        },
        "CentralizedLogging": {
            "type": "object",
            "required": [
                "enabled"
            ],
            "properties": {
                "accountId": {
                    "type": "string",
                    "maxLength": 12,
                    "minLength": 12,
                    "pattern": "^\\d{12}$",
                    "additionalProperties": false
                },
                "configurations": {
                    "$ref": "#/definitions/LoggingConfigurations"
                },
                "enabled": {
                    "type": "boolean",
                    "additionalProperties": false
                }
            },
            "additionalProperties": false,
            "if": {
                "properties": {
                    "enabled": {
                        "const": true
                    }
```

```
                }
            },
            "then": {
                "required": [
                    "accountId"
                ]
            }
        },
        "LoggingConfigurations": {
            "type": "object",
            "properties": {
                "accessLoggingBucket": {
                    "$ref": "#/definitions/S3BucketConfiguration"
                },
                "kmsKeyArn": {
                    "type": "string",
                    "maxLength": 2048,
                    "minLength": 1,
                    "additionalProperties": false
                },
                "loggingBucket": {
                    "$ref": "#/definitions/S3BucketConfiguration"
                }
            },
            "additionalProperties": false
        },
        "S3BucketConfiguration": {
            "type": "object",
            "properties": {
                "retentionDays": {
                    "type": "number",
                    "minimum": 1,
                    "additionalProperties": false
                }
            },
            "additionalProperties": false
        },
        "SecurityRoles": {
            "type": "object",
            "required": [
                "enabled"
            ],
            "properties": {
                "accountId": {
```

```
                    "type": "string",
                    "maxLength": 12,
                    "minLength": 12,
                    "pattern": "^\\d{12}$",
                    "additionalProperties": false
                },
                "enabled": {
                    "type": "boolean",
                    "additionalProperties": false
                }
            },
            "additionalProperties": false,
            "if": {
                "properties": {
                    "enabled": {
                        "const": true
                    }
                }
            },
            "then": {
                "required": [
                    "accountId"
                ]
            }
        },
        "Config": {
            "type": "object",
            "required": [
                "enabled"
            ],
            "properties": {
                "accountId": {
                    "type": "string",
                    "maxLength": 12,
                    "minLength": 12,
                    "pattern": "^\\d{12}$",
                    "additionalProperties": false
                },
                "configurations": {
                    "$ref": "#/definitions/ConfigConfiguration"
                },
                "enabled": {
                    "type": "boolean",
                    "additionalProperties": false
```

```
                }
            },
            "additionalProperties": false,
            "if": {
                "properties": {
                    "enabled": {
                        "const": true
                    }
                }
            },
            "then": {
                "required": [
                    "accountId"
                ]
            }
        },
        "ConfigConfiguration": {
            "type": "object",
            "required": [],
            "properties": {
                "loggingBucket": {
                    "$ref": "#/definitions/S3BucketConfiguration"
                },
                "accessLoggingBucket": {
                    "$ref": "#/definitions/S3BucketConfiguration"
                },
                "kmsKeyArn": {
                    "type": "string",
                    "maxLength": 2048,
                    "minLength": 1,
                    "additionalProperties": false
                }
            }
        }
    }
}
```

Schema der Landezone 3.3

```
{
    "type": "object",
    "required": [
        "centralizedLogging",
```

```
        "organizationStructure",
        "securityRoles"
    ],
    "properties": {
        "accessManagement": {
            "$ref": "#/definitions/AccessManagement"
        },
        "backup": {
            "$ref": "#/definitions/Backup"
        },
        "centralizedLogging": {
            "$ref": "#/definitions/CentralizedLogging"
        },
        "governedRegions": {
            "type": "array",
            "items": {
                "type": "string",
                "maxLength": 24,
                "minLength": 1,
                "pattern": "^[a-z]{2}-[a-z\\-]*-[0-9]{1}$",
                "additionalProperties": false
            },
            "additionalProperties": false
        },
        "organizationStructure": {
            "$ref": "#/definitions/OrganizationStructure"
        },
        "securityRoles": {
            "$ref": "#/definitions/SecurityRoles"
        }
    },
    "additionalProperties": false,
    "definitions": {
        "AccessManagement": {
            "type": "object",
            "required": [
                "enabled"
            ],
            "properties": {
                "enabled": {
                    "type": "boolean",
                    "additionalProperties": false,
                    "default": true
                }
```

```
            },
            "additionalProperties": false
        },
        "Backup": {
            "type": "object",
            "properties": {
                "configurations": {
                    "$ref": "#/definitions/BackupConfigurations"
                },
                "enabled": {
                    "type": "boolean",
                    "additionalProperties": false,
                    "default": false
                }
            },
            "additionalProperties": false,
            "if": {
                "properties": {
                    "enabled": {
                        "const": true
                    }
                }
            },
            "then": {
                "required": [
                    "configurations"
                ]
            }
        },
        "BackupAdminConfigurations": {
            "type": "object",
            "required": [
                "accountId"
            ],
            "properties": {
                "accountId": {
                    "type": "string",
                    "maxLength": 12,
                    "minLength": 12,
                    "pattern": "^\\d{12}$",
                    "additionalProperties": false
                }
            },
            "additionalProperties": false
```

```
        },
        "BackupConfigurations": {
            "type": "object",
            "required": [
                "backupAdmin",
                "centralBackup",
                "kmsKeyArn"
            ],
            "properties": {
                "backupAdmin": {
                    "$ref": "#/definitions/BackupAdminConfigurations"
                },
                "centralBackup": {
                    "$ref": "#/definitions/CentralBackupConfigurations"
                },
                "kmsKeyArn": {
                    "type": "string",
                    "maxLength": 2048,
                    "minLength": 1,
                    "additionalProperties": false
                }
            },
            "additionalProperties": false
        },
        "CentralBackupConfigurations": {
            "type": "object",
            "required": [
                "accountId"
            ],
            "properties": {
                "accountId": {
                    "type": "string",
                    "maxLength": 12,
                    "minLength": 12,
                    "pattern": "^\\d{12}$",
                    "additionalProperties": false
                }
            },
            "additionalProperties": false
        },
        "CentralizedLogging": {
            "type": "object",
            "required": [
                "accountId"
```

```
            ],
            "properties": {
                "accountId": {
                    "type": "string",
                    "maxLength": 12,
                    "minLength": 12,
                    "pattern": "^\\d{12}$",
                    "additionalProperties": false
                },
                "configurations": {
                    "$ref": "#/definitions/LoggingConfigurations"
                },
                "enabled": {
                    "type": "boolean",
                    "additionalProperties": false,
                    "default": true
                }
            },
            "additionalProperties": false
        },
        "LoggingConfigurations": {
            "type": "object",
            "properties": {
                "accessLoggingBucket": {
                    "$ref": "#/definitions/S3BucketConfiguration"
                },
                "kmsKeyArn": {
                    "type": "string",
                    "maxLength": 2048,
                    "minLength": 1,
                    "additionalProperties": false
                },
                "loggingBucket": {
                    "$ref": "#/definitions/S3BucketConfiguration"
                }
            },
            "additionalProperties": false
        },
        "OrganizationalUnit": {
            "type": "object",
            "required": [
                "name"
            ],
            "properties": {
```

```
                "name": {
                    "type": "string",
                    "maxLength": 120,
                    "minLength": 1,
                    "pattern": "^[\\s\\S]*$",
                    "additionalProperties": false
                }
            },
            "additionalProperties": false
        },
        "OrganizationStructure": {
            "type": "object",
            "required": [
                "security"
            ],
            "properties": {
                "sandbox": {
                    "$ref": "#/definitions/OrganizationalUnit"
                },
                "security": {
                    "$ref": "#/definitions/OrganizationalUnit"
                }
            },
            "additionalProperties": false
        },
        "S3BucketConfiguration": {
            "type": "object",
            "properties": {
                "retentionDays": {
                    "type": "number",
                    "minimum": 1,
                    "additionalProperties": false
                }
            },
            "additionalProperties": false
        },
        "SecurityRoles": {
            "type": "object",
            "required": [
                "accountId"
            ],
            "properties": {
                "accountId": {
                    "type": "string",
```

```
                    "maxLength": 12,
                    "minLength": 12,
                    "pattern": "^\\d{12}$",
                    "additionalProperties": false
                }
            },
            "additionalProperties": false
        }
    }
}
```

Schema der Landezone 3.2

```
{
    "type": "object",
    "required": [
        "centralizedLogging",
        "organizationStructure",
        "securityRoles"
    ],
    "properties": {
        "accessManagement": {
            "$ref": "#/definitions/AccessManagement"
        },
        "backup": {
            "$ref": "#/definitions/Backup"
        },
        "centralizedLogging": {
            "$ref": "#/definitions/CentralizedLogging"
        },
        "governedRegions": {
            "type": "array",
            "items": {
                "type": "string",
                "maxLength": 24,
                "minLength": 1,
                "pattern": "^[a-z]{2}-[a-z\\-]*-[0-9]{1}$",
                "additionalProperties": false
            },
            "additionalProperties": false
        },
        "organizationStructure": {
            "$ref": "#/definitions/OrganizationStructure"
```

```
        },
        "securityRoles": {
            "$ref": "#/definitions/SecurityRoles"
        }
    },
    "additionalProperties": false,
    "definitions": {
        "AccessManagement": {
            "type": "object",
            "required": [
                "enabled"
            ],
            "properties": {
                "enabled": {
                    "type": "boolean",
                    "additionalProperties": false,
                    "default": true
                }
            },
            "additionalProperties": false
        },
        "Backup": {
            "type": "object",
            "properties": {
                "configurations": {
                    "$ref": "#/definitions/BackupConfigurations"
                },
                "enabled": {
                    "type": "boolean",
                    "additionalProperties": false,
                    "default": false
                }
            },
            "additionalProperties": false,
            "if": {
                "properties": {
                    "enabled": {
                        "const": true
                    }
                }
            },
            "then": {
                "required": [
                    "configurations"
```

```
                ]
            }
        },
        "BackupAdminConfigurations": {
            "type": "object",
            "required": [
                "accountId"
            ],
            "properties": {
                "accountId": {
                    "type": "string",
                    "maxLength": 12,
                    "minLength": 12,
                    "pattern": "^\\d{12}$",
                    "additionalProperties": false
                }
            },
            "additionalProperties": false
        },
        "BackupConfigurations": {
            "type": "object",
            "required": [
                "backupAdmin",
                "centralBackup",
                "kmsKeyArn"
            ],
            "properties": {
                "backupAdmin": {
                    "$ref": "#/definitions/BackupAdminConfigurations"
                },
                "centralBackup": {
                    "$ref": "#/definitions/CentralBackupConfigurations"
                },
                "kmsKeyArn": {
                    "type": "string",
                    "maxLength": 2048,
                    "minLength": 1,
                    "additionalProperties": false
                }
            },
            "additionalProperties": false
        },
        "CentralBackupConfigurations": {
            "type": "object",
```

```
            "required": [
                "accountId"
            ],
            "properties": {
                "accountId": {
                    "type": "string",
                    "maxLength": 12,
                    "minLength": 12,
                    "pattern": "^\\d{12}$",
                    "additionalProperties": false
                }
            },
            "additionalProperties": false
        },
        "CentralizedLogging": {
            "type": "object",
            "required": [
                "accountId"
            ],
            "properties": {
                "accountId": {
                    "type": "string",
                    "maxLength": 12,
                    "minLength": 12,
                    "pattern": "^\\d{12}$",
                    "additionalProperties": false
                },
                "configurations": {
                    "$ref": "#/definitions/LoggingConfigurations"
                },
                "enabled": {
                    "type": "boolean",
                    "additionalProperties": false,
                    "default": true
                }
            },
            "additionalProperties": false
        },
        "LoggingConfigurations": {
            "type": "object",
            "properties": {
                "accessLoggingBucket": {
                    "$ref": "#/definitions/S3BucketConfiguration"
                },
```

```
                "kmsKeyArn": {
                    "type": "string",
                    "maxLength": 2048,
                    "minLength": 1,
                    "additionalProperties": false
                },
                "loggingBucket": {
                    "$ref": "#/definitions/S3BucketConfiguration"
                }
            },
            "additionalProperties": false
        },
        "OrganizationalUnit": {
            "type": "object",
            "required": [
                "name"
            ],
            "properties": {
                "name": {
                    "type": "string",
                    "maxLength": 120,
                    "minLength": 1,
                    "pattern": "^[\\s\\S]*$",
                    "additionalProperties": false
                }
            },
            "additionalProperties": false
        },
        "OrganizationStructure": {
            "type": "object",
            "required": [
                "security"
            ],
            "properties": {
                "sandbox": {
                    "$ref": "#/definitions/OrganizationalUnit"
                },
                "security": {
                    "$ref": "#/definitions/OrganizationalUnit"
                }
            },
            "additionalProperties": false
        },
        "S3BucketConfiguration": {
```

```
            "type": "object",
            "properties": {
                "retentionDays": {
                    "type": "number",
                    "minimum": 1,
                    "additionalProperties": false
                }
            },
            "additionalProperties": false
        },
        "SecurityRoles": {
            "type": "object",
            "required": [
                "accountId"
            ],
            "properties": {
                "accountId": {
                    "type": "string",
                    "maxLength": 12,
                    "minLength": 12,
                    "pattern": "^\\d{12}$",
                    "additionalProperties": false
                }
            },
            "additionalProperties": false
        }
    }
}
```

Schema der Landezone 3.1

```
{
    "type": "object",
    "required": [
        "centralizedLogging",
        "organizationStructure",
        "securityRoles"
    ],
    "properties": {
        "accessManagement": {
            "$ref": "#/definitions/AccessManagement"
        },
        "backup": {
```

```
            "$ref": "#/definitions/Backup"
        },
        "centralizedLogging": {
            "$ref": "#/definitions/CentralizedLogging"
        },
        "governedRegions": {
            "type": "array",
            "items": {
                "type": "string",
                "maxLength": 24,
                "minLength": 1,
                "pattern": "^[a-z]{2}-[a-z\\-]*-[0-9]{1}$",
                "additionalProperties": false
            },
            "additionalProperties": false
        },
        "organizationStructure": {
            "$ref": "#/definitions/OrganizationStructure"
        },
        "securityRoles": {
            "$ref": "#/definitions/SecurityRoles"
        }
    },
    "additionalProperties": false,
    "definitions": {
        "AccessManagement": {
            "type": "object",
            "required": [
                "enabled"
            ],
            "properties": {
                "enabled": {
                    "type": "boolean",
                    "additionalProperties": false,
                    "default": true
                }
            },
            "additionalProperties": false
        },
        "Backup": {
            "type": "object",
            "properties": {
                "configurations": {
                    "$ref": "#/definitions/BackupConfigurations"
```

```
                },
                "enabled": {
                    "type": "boolean",
                    "additionalProperties": false,
                    "default": false
                }
            },
            "additionalProperties": false,
            "if": {
                "properties": {
                    "enabled": {
                        "const": true
                    }
                }
            },
            "then": {
                "required": [
                    "configurations"
                ]
            }
        },
        "BackupAdminConfigurations": {
            "type": "object",
            "required": [
                "accountId"
            ],
            "properties": {
                "accountId": {
                    "type": "string",
                    "maxLength": 12,
                    "minLength": 12,
                    "pattern": "^\\d{12}$",
                    "additionalProperties": false
                }
            },
            "additionalProperties": false
        },
        "BackupConfigurations": {
            "type": "object",
            "required": [
                "backupAdmin",
                "centralBackup",
                "kmsKeyArn"
            ],
```

```
            "properties": {
                "backupAdmin": {
                    "$ref": "#/definitions/BackupAdminConfigurations"
                },
                "centralBackup": {
                    "$ref": "#/definitions/CentralBackupConfigurations"
                },
                "kmsKeyArn": {
                    "type": "string",
                    "maxLength": 2048,
                    "minLength": 1,
                    "additionalProperties": false
                }
            },
            "additionalProperties": false
        },
        "CentralBackupConfigurations": {
            "type": "object",
            "required": [
                "accountId"
            ],
            "properties": {
                "accountId": {
                    "type": "string",
                    "maxLength": 12,
                    "minLength": 12,
                    "pattern": "^\\d{12}$",
                    "additionalProperties": false
                }
            },
            "additionalProperties": false
        },
        "CentralizedLogging": {
            "type": "object",
            "required": [
                "accountId"
            ],
            "properties": {
                "accountId": {
                    "type": "string",
                    "maxLength": 12,
                    "minLength": 12,
                    "pattern": "^\\d{12}$",
                    "additionalProperties": false
```

```
                },
                "configurations": {
                    "$ref": "#/definitions/LoggingConfigurations"
                },
                "enabled": {
                    "type": "boolean",
                    "additionalProperties": false,
                    "default": true
                }
            },
            "additionalProperties": false
        },
        "LoggingConfigurations": {
            "type": "object",
            "properties": {
                "accessLoggingBucket": {
                    "$ref": "#/definitions/S3BucketConfiguration"
                },
                "kmsKeyArn": {
                    "type": "string",
                    "maxLength": 2048,
                    "minLength": 1,
                    "additionalProperties": false
                },
                "loggingBucket": {
                    "$ref": "#/definitions/S3BucketConfiguration"
                }
            },
            "additionalProperties": false
        },
        "OrganizationalUnit": {
            "type": "object",
            "required": [
                "name"
            ],
            "properties": {
                "name": {
                    "type": "string",
                    "maxLength": 120,
                    "minLength": 1,
                    "pattern": "^[\\s\\S]*$",
                    "additionalProperties": false
                }
            },
```

```
            "additionalProperties": false
        },
        "OrganizationStructure": {
            "type": "object",
            "required": [
                "security"
            ],
            "properties": {
                "sandbox": {
                    "$ref": "#/definitions/OrganizationalUnit"
                },
                "security": {
                    "$ref": "#/definitions/OrganizationalUnit"
                }
            },
            "additionalProperties": false
        },
        "S3BucketConfiguration": {
            "type": "object",
            "properties": {
                "retentionDays": {
                    "type": "number",
                    "minimum": 1,
                    "additionalProperties": false
                }
            },
            "additionalProperties": false
        },
        "SecurityRoles": {
            "type": "object",
            "required": [
                "accountId"
            ],
            "properties": {
                "accountId": {
                    "type": "string",
                    "maxLength": 12,
                    "minLength": 12,
                    "pattern": "^\\d{12}$",
                    "additionalProperties": false
                }
            },
            "additionalProperties": false
        }
```

```
    }
}
```

Starte eine landing zone mit CloudFormation

Sie können eine landing zone CloudFormation entweder über die CloudFormation Konsole oder über die konfigurieren und starten AWS CLI. Dieser Abschnitt enthält Anweisungen und Beispiele zum Starten einer landing zone mithilfe von APIs über CloudFormation.

Themen

- Voraussetzungen für den Start einer landing zone mit CloudFormation
- Erstellen Sie eine neue landing zone mit CloudFormation
- Verwalte eine bestehende landing zone mit CloudFormation

Voraussetzungen für den Start einer landing zone mit CloudFormation

1. Verwenden Sie von der aus die AWS Organizations `CreateOrganization` API AWS CLI, um eine Organisation zu erstellen und alle Funktionen zu aktivieren.

   Genauere Anweisungen finden Sie unterSchritt 1: Konfiguriere deine landing zone.
2. Stellen Sie über die CloudFormation Konsole oder mithilfe der AWS CLI eine CloudFormation Vorlage bereit, mit der die folgenden Ressourcen im Verwaltungskonto erstellt werden:
   - Log Archive-Konto (manchmal auch als „Logging“ -Konto bezeichnet)
   - Auditkonto (manchmal auch als „Sicherheitskonto“ bezeichnet)
   - Die Rollen AWSControlTowerAdminAWSControlTowerCloudTrailRole, AWSControlTowerConfigAggregatorRoleForOrganizations, und AWSControlTowerStackSetRoleService.

     Informationen darüber, wie AWS Control Tower diese Rollen verwendet, um Landingzone-API-Aufrufe durchzuführen, finden Sie unter Schritt 1: Konfiguration Ihrer landing zone.

```
Parameters:
  LoggingAccountEmail:
    Type: String
    Description: The email Id for centralized logging account
  LoggingAccountName:
    Type: String
    Description: Name for centralized logging account
```

```
  SecurityAccountEmail:
    Type: String
    Description: The email Id for security roles account
  SecurityAccountName:
    Type: String
    Description: Name for security roles account
Resources:
  MyOrganization:
    Type: 'AWS::Organizations::Organization'
    Properties:
      FeatureSet: ALL
  LoggingAccount:
    Type: 'AWS::Organizations::Account'
    Properties:
      AccountName: !Ref LoggingAccountName
      Email: !Ref LoggingAccountEmail
  SecurityAccount:
    Type: 'AWS::Organizations::Account'
    Properties:
      AccountName: !Ref SecurityAccountName
      Email: !Ref SecurityAccountEmail
  AWSControlTowerAdmin:
    Type: 'AWS::IAM::Role'
    Properties:
      RoleName: AWSControlTowerAdmin
      AssumeRolePolicyDocument:
        Version: 2012-10-17
        Statement:
          - Effect: Allow
            Principal:
              Service: controltower.amazonaws.com
            Action: 'sts:AssumeRole'
      Path: '/service-role/'
      ManagedPolicyArns:
        - !Sub >-
          arn:${AWS::Partition}:iam::aws:policy/service-role/
AWSControlTowerServiceRolePolicy
  AWSControlTowerAdminPolicy:
    Type: 'AWS::IAM::Policy'
    Properties:
      PolicyName: AWSControlTowerAdminPolicy
      PolicyDocument:
        Version: 2012-10-17
        Statement:
```

```
          - Effect: Allow
            Action: 'ec2:DescribeAvailabilityZones'
            Resource: '*'
      Roles:
        - !Ref AWSControlTowerAdmin
  AWSControlTowerCloudTrailRole:
    Type: 'AWS::IAM::Role'
    Properties:
      RoleName: AWSControlTowerCloudTrailRole
      AssumeRolePolicyDocument:
        Version: 2012-10-17
        Statement:
          - Effect: Allow
            Principal:
              Service: cloudtrail.amazonaws.com
            Action: 'sts:AssumeRole'
      Path: '/service-role/'
  AWSControlTowerCloudTrailRolePolicy:
    Type: 'AWS::IAM::Policy'
    Properties:
      PolicyName: AWSControlTowerCloudTrailRolePolicy
      PolicyDocument:
        Version: 2012-10-17
        Statement:
          - Action:
              - 'logs:CreateLogStream'
              - 'logs:PutLogEvents'
            Resource: !Sub >-
              arn:${AWS::Partition}:logs:*:*:log-group:aws-controltower/
CloudTrailLogs:*
            Effect: Allow
      Roles:
        - !Ref AWSControlTowerCloudTrailRole
  AWSControlTowerConfigAggregatorRoleForOrganizations:
    Type: 'AWS::IAM::Role'
    Properties:
      RoleName: AWSControlTowerConfigAggregatorRoleForOrganizations
      AssumeRolePolicyDocument:
        Version: 2012-10-17
        Statement:
          - Effect: Allow
            Principal:
              Service: config.amazonaws.com
            Action: 'sts:AssumeRole'
```

```
      Path: '/service-role/'
      ManagedPolicyArns:
        - !Sub arn:${AWS::Partition}:iam::aws:policy/service-role/
AWSConfigRoleForOrganizations
  AWSControlTowerStackSetRole:
    Type: 'AWS::IAM::Role'
    Properties:
      RoleName: AWSControlTowerStackSetRole
      AssumeRolePolicyDocument:
        Version: 2012-10-17
        Statement:
          - Effect: Allow
            Principal:
              Service: cloudformation.amazonaws.com
            Action: 'sts:AssumeRole'
      Path: '/service-role/'
  AWSControlTowerStackSetRolePolicy:
    Type: 'AWS::IAM::Policy'
    Properties:
      PolicyName: AWSControlTowerStackSetRolePolicy
      PolicyDocument:
        Version: 2012-10-17
        Statement:
          - Action: 'sts:AssumeRole'
            Resource: !Sub 'arn:${AWS::Partition}:iam::*:role/
AWSControlTowerExecution'
            Effect: Allow
      Roles:
        - !Ref AWSControlTowerStackSetRole

Outputs:
  LogAccountId:
    Value:
      Fn::GetAtt: LoggingAccount.AccountId
    Export:
      Name: LogAccountId
  SecurityAccountId:
    Value:
      Fn::GetAtt: SecurityAccount.AccountId
    Export:
      Name: SecurityAccountId
```

Erstellen Sie eine neue landing zone mit CloudFormation

Stellen Sie über die CloudFormation Konsole oder mithilfe der die folgende CloudFormation Vorlage bereit AWS CLI, um eine landing zone zu erstellen.

```
Parameters:
  Version:
    Type: String
    Description: The version number of Landing Zone
  GovernedRegions:
    Type: CommaDelimitedList
    Description: List of governed regions
  SecurityOuName:
    Type: String
    Description: The security Organizational Unit name
  SandboxOuName:
    Type: String
    Description: The sandbox Organizational Unit name
  CentralizedLoggingAccountId:
    Type: String
    Description: The AWS account ID for centralized logging
  SecurityAccountId:
    Type: String
    Description: The AWS account ID for security roles
  LoggingBucketRetentionPeriod:
    Type: Number
    Description: Retention period for centralized logging bucket
  AccessLoggingBucketRetentionPeriod:
    Type: Number
    Description: Retention period for access logging bucket
  KMSKey:
    Type: String
    Description: KMS key ARN used by CloudTrail and Config service to encrypt data in
 logging bucket
Resources:
  MyLandingZone:
    Type: 'AWS::ControlTower::LandingZone'
    Properties:
      Version:
        Ref: Version
      Tags:
        - Key: "keyname1"
          Value: "value1"
```

```
      - Key: "keyname2"
        Value: "value2"
    Manifest:
      governedRegions:
        Ref: GovernedRegions
      organizationStructure:
        security:
          name:
            Ref: SecurityOuName
        sandbox:
          name:
            Ref: SandboxOuName
      centralizedLogging:
        accountId:
          Ref: CentralizedLoggingAccountId
        configurations:
          loggingBucket:
            retentionDays:
              Ref: LoggingBucketRetentionPeriod
          accessLoggingBucket:
            retentionDays:
              Ref: AccessLoggingBucketRetentionPeriod
          kmsKeyArn:
            Ref: KMSKey
        enabled: true
      securityRoles:
        accountId:
          Ref: SecurityAccountId
      accessManagement:
        enabled: true
```

Verwalte eine bestehende landing zone mit CloudFormation

Sie können CloudFormation damit eine landing zone verwalten, die Sie bereits gestartet haben, indem Sie die landing zone in einen neuen oder vorhandenen CloudFormation Stack importieren. Einzelheiten und Anweisungen finden Sie unter Einbindung vorhandener Ressourcen in die CloudFormation Verwaltung.

Um Abweichungen innerhalb einer landing zone zu erkennen und zu beheben, können Sie die AWS Control Tower Tower-Konsole AWS CLI, die oder die `ResetLandingZone`API verwenden.

Nächste Schritte

Jetzt, da Ihre Landezone eingerichtet ist, ist sie einsatzbereit.

Weitere Informationen zur Verwendung von AWS Control Tower finden Sie in den folgenden Themen:

- Empfohlene administrative Vorgehensweisen finden Sie unter Bewährte Methoden.
- Sie können IAM Identity Center-Benutzer und -Gruppen mit bestimmten Rollen und Berechtigungen einrichten. Entsprechende Empfehlungen finden Sie unter Empfehlungen für die Einrichtung von Gruppen, Rollen und Richtlinien.
- Wie Sie mit der Registrierung von Organisationen und Konten aus Ihren AWS Organizations Bereitstellungen beginnen, finden Sie unter Steuern vorhandener Organisationen und Konten.
- Ihre Endbenutzer können mithilfe von Account Factory ihre eigenen AWS Konten in Ihrer Landing Zone einrichten. Weitere Informationen finden Sie unter Berechtigungen für die Konfiguration und Bereitstellung von Konten.
- Um dies sicherzustellenKonformitätsvalidierung für AWS Control Tower, können Ihre zentralen Cloud-Administratoren die Protokollarchive im Log Archive-Konto überprüfen, und bestimmte externe Auditoren können die Auditinformationen im Audit-Konto (gemeinsam genutzt) überprüfen, das ein Mitglied der Security OU ist.
- Weitere Informationen zu den Funktionen von AWS Control Tower finden Sie unter Verwandte Informationen.
- Von Zeit zu Zeit müssen Sie möglicherweise Ihre Landezone aktualisieren, um die neuesten Backend-Updates und die neuesten Steuerelemente zu erhalten und Ihre Landezone auf dem neuesten Stand zu halten. Weitere Informationen finden Sie unter Verwaltung von Konfigurationsupdates in AWS Control Tower.
- Wenn Sie bei der Verwendung von AWS Control Tower auf Probleme stoßen, finden Sie weitere Informationen unterFehlerbehebung.

> **Important**
>
> Wenn Sie MFA für den Root-Benutzer Ihres Kontos noch nicht aktiviert haben, tun Sie dies jetzt. Weitere Informationen zu bewährten Methoden für den Root-Benutzer finden Sie unter Bewährte Methoden zum Schutz des Root-Benutzers Ihres Kontos.

Einschränkungen und Kontingente in AWS Control Tower

In diesem Kapitel werden die AWS Servicebeschränkungen und Kontingente behandelt, die Sie bei der Verwendung von AWS Control Tower berücksichtigen sollten. Wenn Sie Ihre Landezone aufgrund eines Problems mit der Servicequote nicht einrichten können, wenden Sie sich an AWS Support.

Weitere Informationen zu Einschränkungen, die sich speziell auf Steuerelemente beziehen, finden Sie unterEinschränkungen bei der Steuerung.

> **Das Referenzhandbuch für Steuerelemente**
>
> Detaillierte Informationen zu den Steuerungen von AWS Control Tower wurden in den Referenzleitfaden für AWS Control Tower Controls verschoben.

Bekannte Einschränkungen in AWS Control Tower

In diesem Abschnitt werden bekannte Einschränkungen und nicht unterstützte Anwendungsfälle in AWS Control Tower beschrieben.

- Für AWS Control Tower gelten allgemeine Einschränkungen bei der Parallelität. Im Allgemeinen ist eine Operation nach der anderen zulässig. Zwei Ausnahmen von dieser Einschränkung sind zulässig:
  - Optionale Steuerelemente können durch einen asynchronen Prozess gleichzeitig aktiviert und deaktiviert werden. Insgesamt können bis zu einhundert (100) steuerelementbezogene Operationen gleichzeitig ausgeführt werden, unabhängig davon, ob sie von der Konsole oder von einer API aus aufgerufen werden.
  - Konten können über einen asynchronen Prozess gleichzeitig in Account Factory bereitgestellt, aktualisiert und registriert werden, wobei bis zu fünf (5) kontobezogene Vorgänge gleichzeitig ausgeführt werden. Die Kontoverwaltung muss für jedes Konto einzeln aufgehoben werden.
    - Wenn die automatische Registrierung aktiviert ist, kann nur ein einziger Kontoverschiebungsvorgang für die Ziel-Organisationseinheit ausgeführt werden. Alle weiteren kontobezogenen Vorgänge in derselben Organisationseinheit gelten als widersprüchlich, bis der Vorgang zum Verschieben des Kontos abgeschlossen ist.

  - In Account Factory for Terraform (AFT) werden während der Bereitstellung zusätzliche Parallelitätsparameter konfiguriert. AWS hat AFT mit diesen Standardwerten getestet:
    - `concurrent_account_factory_actions`: 5 (Kontobereitstellung)
    - `maximum_concurrent_customizations`: 5 (Pipelines zur Anpassung)

    Eine Erhöhung dieser Grenzwerte über die getesteten Standardwerte hinaus kann die Stabilität beeinträchtigen.
- Die E-Mail-Adressen von gemeinsam genutzten Konten in der Security OU können geändert werden. Sie müssen jedoch Ihre Landing Zone aktualisieren, damit diese Änderungen in der AWS Control Tower-Konsole angezeigt werden.
- Für OUs in Ihrer AWS Control Tower-Landezone gilt ein Limit von zehn (10) SCPs pro OU.
- AWS Control Tower unterstützt bis zu 10.000 Konten in der Organisation Ihrer Landing Zone, aufgeteilt auf alle Ihre OUs.
- Bestehende OUs mit über 1000 direkt verschachtelten Konten können im AWS Control Tower nicht registriert oder erneut registriert werden. Weitere Informationen zu Einschränkungen bei der Registrierung von Organisationseinheiten finden Sie unter. Einschränkungen, die auf dem zugrunde liegenden Grund basieren AWS service
- Anpassungen für AWS Control Tower (cFCT) sind in diesen nicht verfügbar AWS-Regionen, da einige Abhängigkeiten nicht verfügbar sind:
  - Europa (Zürich), eu-central-2
  - Europa (Spanien), eu-Süd-2
  - Westkanada (Calgary) ca-west-1
  - Asien-Pazifik (Melbourne), AP-Southeast-4
  - Asien-Pazifik (Malaysia), AP-Southeast-5
  - Asien-Pazifik (Thailand), ap-southeast-7
  - Mexiko (Zentral), mx-central-1
  - Asien-Pazifik (Neuseeland), ap-southeast-6
  - Asien-Pazifik (Taipeh), ap-east-2
  - AWS European Sovereign Cloud (Deutschland), eusc-de-east-1

  Sie können Ressourcen in diesen Regionen mit cFCT bereitstellen und verwalten, wenn Sie cFCT in Ihrer AWS Control Tower-Heimatregion bereitstellen, aber Sie können cFCT in diesen Regionen nicht erstellen.

- AWS Control Tower Account Factory for Terraform (AFT) ist in den folgenden Ländern nicht verfügbar AWS-Regionen, da einige Abhängigkeiten nicht verfügbar sind:
  - Europa (Zürich), eu-central-2
  - Europa (Spanien), eu-Süd-2
  - Westkanada (Calgary), ca-west-1
  - Asien-Pazifik (Melbourne), AP-Southeast-4
  - Asien-Pazifik (Malaysia), AP-Southeast-5
  - Asien-Pazifik (Thailand), ap-southeast-7
  - Mexiko (Zentral), mx-central-1
  - Asien-Pazifik (Neuseeland), ap-southeast-6
  - Asien-Pazifik (Taipeh), ap-east-2
  - AWS European Sovereign Cloud (Deutschland), eusc-de-east-1
- AWS Control Tower Account Factory for Terraform (AFT) kann von neuen AFT-Kunden in den folgenden Regionen nicht bereitgestellt werden, da keine Verbindung zu einem AWS CodeConnections Versionskontrollsystem (VCS) eines Drittanbieters hergestellt werden kann:
  - Asien-Pazifik (Hongkong), Afrika (Kapstadt), Naher Osten (Bahrain), Europa (Zürich), Asien-Pazifik (Jakarta), Asien-Pazifik (Hyderabad), Asien-Pazifik (Osaka), Asien-Pazifik (Melbourne), Israel (Tel Aviv), Europa (Spanien), Naher Osten (VAE), Asien-Pazifik (Thailand), Mexiko (Zentral)
- Die folgenden Regionen unterstützen nicht. AWS Service Catalog
  - Kanada West (Calgary), ca-west-1
  - Asien-Pazifik (Malaysia), AP-Southeast-5
  - Asien-Pazifik (Thailand), ap-southeast-7
  - Mexiko (Zentral), mx-central-1
  - Asien-Pazifik (Neuseeland), ap-southeast-6
  - Asien-Pazifik (Taipeh), ap-east-2
  - AWS European Sovereign Cloud (Deutschland), eusc-de-east-1

> **Note**
>
> Regionen, die Service Catalog nicht unterstützen, unterstützen keine Account Factory-Anpassungen für AWS Control Tower (AFC).

Weitere Informationen zur AWS Control Tower-Funktionalität in Regionen, die dies nicht unterstützen AWS Service Catalog, finden Sie unter. AWS Control Tower ist verfügbar in AWS Kanada West (Calgary)

- Wenn Sie eine Kontroll-API aufrufen, um eine Steuerung zu aktivieren oder zu deaktivieren, liegt das Limit für `EnableControl` und `DisableControl` Aktualisierungen im AWS Control Tower bei einhundert (100) gleichzeitigen Vorgängen. Zehn Operationen (10) können gleichzeitig ausgeführt werden, wobei die verbleibenden Operationen in die Warteschlange gestellt werden. Möglicherweise müssen Sie Ihren Code anpassen, um auf den Abschluss zu warten.
- Wenn Sie Konten über Account Factory Customizations (AFC) mit Blueprints bereitstellen, die auf Terraform basieren, können Sie diese Blueprints nur für einen bereitstellen. AWS-Region Standardmäßig wird AWS Control Tower in der Heimatregion bereitgestellt.

Anfordern einer Kontingenterhöhung

Die Service Quotas Console bietet Informationen zu AWS Control Tower-Kontingenten. Sie können die Service Quota-Konsole verwenden, um die Standard-Servicekontingente einzusehen oder um Kontingenterhöhungen für anpassbare Kontingente anzufordern.

> **Note**
>
> Bei neu erstellten Konten und Organisationen liegt das Kontingent möglicherweise unter dem Standardwert von 10 Konten.

Die folgenden Kontingente können über die Service Quota-Konsole eingesehen werden

- Kontingent für gleichzeitige Kontovorgänge: Die maximale Anzahl gleichzeitiger Kontovorgänge, die gleichzeitig ausgeführt werden können. Standard: 5, Maximum: 10, einstellbar
- Anzahl der Konten in einer einzelnen OU: Die maximale Anzahl der von AWS Control Tower verwalteten Konten, die in einer OU vorhanden sein können. Wenn Sie Konten hinzufügen, die dieses Limit überschreiten, kann der OU-Registrierungsprozess im AWS Control Tower nicht durchgeführt werden. Weitere Informationen zur Anzahl der Konten pro OU finden Sie Einschränkungen, die auf dem zugrunde liegenden Grund basieren AWS service in der AWS Control Tower-Dokumentation. Standard: 1000, nicht einstellbar.

- Gleichzeitige Operationen für Organisationseinheiten (OUs): Die maximale Anzahl gleichzeitiger OU-related Vorgänge, die gleichzeitig ausgeführt werden können. Standard: 1, nicht einstellbar.

Sie können beispielsweise eine Kontingenterhöhung für fünf von bis zu zehn gleichzeitigen kontobezogenen Vorgängen beantragen. Einige Leistungsmerkmale von AWS Control Tower können sich nach einer Kontingenterhöhung ändern. Beispielsweise kann es länger dauern, eine OU zu aktualisieren, wenn Sie mehr Konten darin haben. Oder es kann länger dauern, eine Aktion an einer OU mit fünf SCPs abzuschließen als mit drei SCPs.

> **Note**
>
> Eine Anfrage zur Erhöhung des Servicekontingents kann bis zu zwei Tage dauern, bis sie wirksam wird. Stellen Sie sicher, dass Sie die Kontingenterhöhung in Ihrer AWS Control Tower-Heimatregion beantragen.

Als Alternative können Sie sich an den AWS Support wenden, um eine Kontingenterhöhung für einige Ressourcen im AWS Control Tower anzufordern. Oder Sie können sich das folgende Video ansehen und erfahren, wie Sie bestimmte Erhöhungen der Servicekontingente automatisieren können.

Video: Automatisieren Sie Anfragen zur Erhöhung der Servicekontingente für Services im Zusammenhang mit AWS Control Tower

In diesem Video (7:24) wird beschrieben, wie die Erhöhung der Servicequoten für verwandte, integrierte AWS Services auf der Grundlage von Bereitstellungen im AWS Control Tower automatisiert werden kann. Es zeigt auch, wie Sie die Registrierung neuer Konten beim AWS Enterprise Support für Ihr Unternehmen automatisieren können. Wählen Sie zur besseren Ansicht das Symbol in der rechten unteren Ecke des Videos, um es in voller Bildschirmgröße anzuzeigen. Es stehen Untertitel zur Verfügung.

Videoanleitung zur Erhöhung der Kontingente im AWS Control Tower.

Bei der Bereitstellung neuer Konten in dieser Umgebung können Sie Lebenszyklusereignisse verwenden, um automatische Anfragen zur Erhöhung des Servicekontingents in bestimmten AWS-Regionen Fällen auszulösen.

Weitere Informationen zu AWS Kontingenten finden Sie in der AWS Allgemeinen Referenz.

Einschränkungen bei der Steuerung

AWS Control Tower unterstützt Sie bei der Aufrechterhaltung einer sicheren Umgebung mit mehreren Konten mithilfe AWS von Kontrollen, die in verschiedenen Formen implementiert werden, z. B. Service Control Policies (SCPs), AWS Config Regeln und CloudFormation Hooks.

> **Das Referenzhandbuch für Steuerelemente**
>
> Detaillierte Informationen zu den Steuerungen von AWS Control Tower wurden in den Referenzleitfaden für AWS Control Tower Controls verschoben.

Wenn Sie AWS Control Tower-Ressourcen, wie z. B. einen SCP, ändern oder eine AWS Config Ressource wie einen Config-Recorder oder Aggregator entfernen, kann AWS Control Tower nicht mehr garantieren, dass die Steuerungen wie vorgesehen funktionieren. Daher kann die Sicherheit Ihrer Umgebung mit mehreren Konten gefährdet sein. Das Sicherheitsmodell der AWS geteilten Verantwortung gilt für alle derartigen Änderungen, die Sie vornehmen.

> **Note**
>
> AWS Control Tower trägt zur Aufrechterhaltung der Integrität Ihrer Umgebung bei, indem die SCPs der präventiven Kontrollen auf ihre Standardkonfiguration zurückgesetzt werden, wenn Sie Ihre Landezone aktualisieren. Änderungen, die Sie möglicherweise an SCPs vorgenommen haben, werden standardmäßig durch die Standardversion der Steuerung ersetzt.

Einschränkungen nach Regionen

Einige Steuerungen im AWS Control Tower funktionieren in bestimmten Ländern, in AWS-Regionen denen AWS Control Tower verfügbar ist, nicht, da diese Regionen die erforderlichen grundlegenden Funktionen nicht unterstützen. Wenn Sie diese Steuerung bereitstellen, funktioniert sie daher möglicherweise nicht in allen Regionen, die Sie mit dem AWS Control Tower verwalten. Diese Einschränkung betrifft bestimmte Detektivkontrollen, bestimmte proaktive Kontrollen und bestimmte Kontrollen im Security Hub Service-managed CSPM-Standard: AWS Control Tower. Weitere Informationen zur regionalen Verfügbarkeit finden Sie in den Security Hub-Steuerelementen. Weitere Informationen finden Sie in der Dokumentation zur Liste der regionalen Dienste und in der Referenzdokumentation zu den Security Hub CSPM-Steuerelementen.

Bei gemischter Steuerung ist das Kontrollverhalten ebenfalls eingeschränkt. Weitere Informationen finden Sie unter Vermeiden Sie eine gemischte Steuerung bei der Konfiguration von Regionen.

Weitere Informationen darüber, wie AWS Control Tower mit den Einschränkungen von Regionen und Kontrollen umgeht, finden Sie unterÜberlegungen zur Aktivierung AWS Opt-in-Regionen.

> **Note**
>
> Für die aktuellsten Informationen zu Kontrollen und Regionsunterstützung empfehlen wir Ihnen, die `ListControls` API-Operationen `GetControl` und aufzurufen.

Finden Sie verfügbare Steuerelemente und Regionen

Sie können die verfügbaren Regionen für jedes Steuerelement in der AWS Control Tower-Konsole einsehen. Sie können die verfügbaren Regionen programmgesteuert mit den `ListControls` APIs `GetControl` und aus AWS Control Catalog anzeigen.

Informationen zu AWS Security Hub CSPM Kontrollen aus dem Service-Managed Standard: AWS Control Tower, die in bestimmten Regionen nicht unterstützt werden AWS-Regionen, finden Sie im Security Hub CSPM-Standard unter „Nicht unterstützte Regionen“.

Einschränkungen, die auf dem zugrunde liegenden Grund basieren AWS service

Auf dieser Seite werden Einschränkungen beschrieben, auf die Sie aufgrund von Einschränkungen bei anderen AWS Diensten stoßen können, und wie AWS Control Tower mit diesen Diensten zusammenarbeitet.

Allgemeine Richtlinien

In der Regel gehen wir davon aus, dass die Anzahl der Konten, die bei der Registrierung einer Organisationseinheit unterstützt werden, abnimmt, wenn Sie die Anzahl der verwalteten Regionen und die Anzahl der aktivierten Kontrollen für diese Organisationseinheit erhöhen. Bei diesen allgemeinen Richtlinien wird davon ausgegangen, dass Sie 15 optionale Steuerelemente aktiviert haben. Wenn Sie mehr oder weniger Steuerelemente in Ihrer Organisationseinheit aktiviert haben, unterscheiden sich die Beschränkungen für Konten pro Organisationseinheit bei der Registrierung.

- In 15 regulierten Regionen werden Organisationseinheiten mit bis zu 1000 Konten unterstützt.

- Bei 16 bis 21 verwalteten Regionen liegt die maximal unterstützte OU-Größe im Bereich von 600—1000 Konten.
- Bei 22 verwalteten Regionen werden Organisationseinheiten mit bis zu 680 Konten unterstützt.
- Bei 23 oder mehr verwalteten Regionen liegt die maximal unterstützte OU-Größe bei weniger als 680 Konten.

Im Falle eines Fehlers

Wenn die Registrierung fehlschlägt, können Sie es mit Re-register der OU versuchen. Sie können die Organisationseinheit auch verkleinern, indem Sie eine verschachtelte Organisationseinheit verwenden oder Konten in eine andere Organisationseinheit verschieben.

> **Note**
>
> Die obligatorischen Kontrollen, die AWS Control Tower immer durchsetzt, werden nicht auf die Anzahl der Kontrollen angerechnet, die Sie für die Registrierung auf einer OU aktiviert haben.

CloudFormation Stack-Set-Einschränkungen

Wenn Sie vorhaben, eine große Anzahl von Konten auf mehreren Konten zu registrieren AWS-Regionen, stoßen Sie möglicherweise auf Beschränkungen, die durch CloudFormation Stacksets für die Gesamtgröße einer Organisation festgelegt werden. Sie können die Limitierung mit dieser Formel abschätzen:

Anzahl der verwalteten Konten in der Organisation x Anzahl der verwalteten Regionen <= 150.000

Diese Einschränkung wird bei der Registrierung einer Organisationseinheit deutlich. Wenn beispielsweise 15 Regionen verwaltet werden und 15 optionale Steuerelemente aktiviert sind, liegt das Limit für die Registrierung der OU bei 1000 Konten. Wenn Sie jedoch Organisationseinheiten mit mehr als 1000 Konten registrieren müssen oder wenn Sie eine große Anzahl optionaler Steuerelemente aktiviert haben, müssen Sie die Anzahl der verwalteten Regionen unter 15 reduzieren. Diese Reduzierung ist auf die Einschränkungen des Stack-Sets zurückzuführen.

AWS Config Einschränkungen

Wenn Sie planen, OUs mit einer großen Anzahl von Konten zu registrieren, kann es sein, dass die maximale Anzahl von Konten, die jede Woche erstellt oder gelöscht werden AWS Config können, auf

allen Aggregatoren begrenzt ist. Registrierte Konten zählen nicht zu diesem Limit: Sie können jede Woche bis zu 1000 neue Konten bei AWS Control Tower registrieren.

First-time Einschränkungen für Konten und Opt-in-Regionen

Wenn Sie planen, OUs zum ersten Mal mit einer großen Anzahl von Konten in mehreren Opt-in-Regionen zu registrieren, können Sie aufgrund von Kontingenten in der Kontoverwaltung auf Einschränkungen stoßen, die zu einer längeren Latenz führen können. Aufgrund der Latenz können bei der Registrierung einer Organisationseinheit Fehler auftreten.

Regionale Unterschiede bei der AWS Control Tower-Funktionalität

Es gibt gewisse Unterschiede im Verhalten von AWS Control Tower AWS-Regionen, da AWS Control Tower das Verhalten anderer AWS Dienste orchestriert. Beispiel:

- AWS Service Catalog ist nicht überall dort verfügbar, AWS-Regionen wo AWS Control Tower verfügbar ist, was das Verhalten von Account Factory in diesen Regionen verändert.
- In bestimmten Regionen ist Account Factory Customizations (AFC) nicht verfügbar, da Service Catalog nicht verfügbar ist, um die zugrunde liegenden Funktionen für Blueprints zu unterstützen.
- Bestimmte Steuerelemente sind AWS-Regionen aufgrund fehlender zugrundeliegender Funktionen nicht in allen Bereichen verfügbar.
- AFT und CFCT sind AWS-Regionen aufgrund fehlender zugrundeliegender Funktionen nicht in allen verfügbar.

Ermitteln Sie Ihre Heimatregion, um das Verhalten Ihrer AWS Control Tower-Umgebung bestmöglich zu bestimmen. Bewerten Sie dann die folgenden Punkte. Weitere Informationen finden Sie unter Einschränkungen und Kontingente in AWS Control Tower.

- Ist in Ihrer gewünschten Heimatregion AWS Service Catalog verfügbar?
- Sind die Steuerungen verfügbar, die Sie benötigen? Siehe Einschränkungen bei der Steuerung.
- Ist IAM Identity Center in Ihrer gewünschten Heimatregion verfügbar?

Bereitstellbare Regionen für Kontrollen

AWS Control Tower kann bestimmte Steuerelemente nicht aktivieren, wenn Sie sie in bestimmten Regionen bereitstellen, da keine zugrunde liegenden Abhängigkeiten vorliegen. Die aktuellsten Informationen zu den bereitstellbaren Regionen für jedes Steuerelement finden Sie, indem Sie die

`GetControl` APIs `ListControls` und aufrufen. Sie können die bereitstellbaren Regionen auch in der AWS Control Tower-Konsole einsehen.

Wenn Sie eine Steuerung auf einer OU aktivieren, die vom AWS Control Tower gesteuert wird, ist der effektive Bereich der Kontrolle der Schnittpunkt Ihrer vom AWS Control Tower gesteuerten Regionen mit den bereitstellbaren Regionen der Steuerung.

Beispielsweise kann ein Steuerelement auf einer OU aktiviert werden, die in den kontrollierten Regionen X, Y und Z betrieben wird. Nach der Aktivierung wird dasselbe Steuerelement jedoch nur in den Regionen X und Z bereitgestellt, da das Steuerelement selbst die Region Y nicht unterstützt.

Es ist wichtig, die Beziehungen zwischen den von Ihnen bereitgestellten Kontrollen und den Regionen, in denen Sie Workloads im AWS Control Tower ausführen, zu überwachen, damit es beim Schutz Ihrer AWS Ressourcen nicht zu Lücken kommt.

So überprüfen Sie Ihre geschützten Regionen

- In der AWS Control Tower-Konsole können Sie die aktivierten Steuerungen und Regionen im Abschnitt Aktivierte Steuerelemente einsehen.
- Wenn Sie die `GetEnabledControl` API aufrufen, zeigt der Parameter targetRegions nur die Regionen an, in denen Sie die Steuerung effektiv einsetzen können, nicht die Regionen, die nicht bereitgestellt werden können.

Das Referenzhandbuch zu AWS Control Tower Controls

Detaillierte Informationen zu den Steuerungen im AWS Control Tower wurden in den Referenzleitfaden für AWS Control Tower Controls verschoben .

Bewährte Methoden für AWS Control Tower Tower-Administratoren

Dieses Thema richtet sich in erster Linie an Administratoren von Verwaltungskonten.

Administratoren von Verwaltungskonten sind dafür verantwortlich, einige Aufgaben zu erklären, die ihre Mitgliedskontenadministratoren aufgrund von AWS Control Tower Tower-Kontrollen nicht ausführen können. In diesem Thema werden einige bewährte Methoden und Verfahren für die Weitergabe dieses Wissens beschrieben. Außerdem finden Sie weitere Tipps für die effiziente Einrichtung und Wartung Ihrer AWS Control Tower Tower-Umgebung.

Erläuterung des Zugriffs für Benutzer

Die AWS Control Tower Tower-Konsole ist nur für Benutzer mit Administratorrechten für das Verwaltungskonto verfügbar. Nur diese Benutzer können administrative Arbeiten in Ihrer landing zone ausführen. Gemäß den bewährten Methoden bedeutet dies, dass die Mehrheit Ihrer Benutzer und Mitgliedskontenadministratoren die AWS Control Tower Tower-Konsole niemals sehen wird. Als Mitglied der Administratorgruppe für Verwaltungskonten liegt es in Ihrer Verantwortung, den Benutzern und Administratoren Ihrer Mitgliedskonten gegebenenfalls die folgenden Informationen zu erläutern.

- Erläutern Sie, auf welche AWS Ressourcen Benutzer und Administratoren in der landing zone Zugriff haben.
- Führen Sie die präventiven Kontrollen auf, die für jede Organisationseinheit (OU) gelten, damit die anderen Administratoren ihre AWS Workloads entsprechend planen und ausführen können.

Erläuterung des Ressourcenzugriffs

Einige Administratoren und andere Benutzer benötigen möglicherweise eine Erklärung der AWS Ressourcen, auf die sie in Ihrer landing zone Zugriff haben. Hierzu können programmgesteuerter Zugriff und konsolenbasierter Zugriff gehören. Im Allgemeinen ist Lese- und Schreibzugriff auf AWS Ressourcen zulässig. Um dort arbeiten zu können AWS, benötigen Ihre Benutzer einen gewissen Zugriff auf die spezifischen Dienste, die sie für ihre Arbeit benötigen.

Einige Benutzer, wie z. B. Ihre AWS Entwickler, müssen möglicherweise wissen, auf welche Ressourcen sie Zugriff haben, damit sie technische Lösungen entwickeln können. Andere Benutzer,

z. B. die Endbenutzer der Anwendungen, die auf AWS Diensten ausgeführt werden, müssen nichts über AWS Ressourcen in Ihrer landing zone wissen.

AWS bietet Tools, mit denen Sie den Umfang des AWS Ressourcenzugriffs eines Benutzers ermitteln können. Nachdem Sie den Umfang des Zugriffs eines Benutzers identifiziert haben, können Sie diese Informationen gemäß den Informationsverwaltungsrichtlinien Ihrer Organisation für den Benutzer freigeben. Weitere Informationen zu diesen Tools finden Sie über die folgenden Links.

- AWS Access Advisor — Mit dem Access Advisor-Tool AWS Identity and Access Management (IAM) können Sie die Berechtigungen Ihrer Entwickler ermitteln, indem Sie den letzten Zeitstempel analysieren, zu dem eine IAM-Entität, z. B. ein Benutzer, eine Rolle oder eine Gruppe, einen Dienst aufgerufen hat. AWS Sie können den Servicezugriff überwachen und unnötige Berechtigungen entfernen und den Prozess bei Bedarf automatisieren. Weitere Informationen finden Sie in unserem Blogbeitrag zum Thema AWS Sicherheit.
- IAM-Richtliniensimulator — Mit dem IAM-Richtliniensimulator können Sie ressourcenbasierte Richtlinien testen IAM-based und Fehler beheben. Weitere Informationen finden Sie unter Testen von IAM-Richtlinien mit dem IAM-Richtliniensimulator.
- AWS CloudTrail Protokolle — Sie können die AWS CloudTrail Protokolle überprüfen, um zu sehen, welche Aktionen von einem Benutzer, einer Rolle oder ausgeführt wurden. AWS-Service Weitere Informationen zu CloudTrail finden Sie im AWS CloudTrail Benutzerhandbuch.

  Die von den Administratoren der AWS Control Tower landing zone ergriffenen Aktionen sind im landing zone Zone-Verwaltungskonto einsehbar. Die von den Administratoren und Benutzern von Mitgliedskonten ergriffenen Aktionen sind im gemeinsamen Protokollarchiv-Konto einsehbar.

  Eine Übersichtstabelle der AWS Control Tower Tower-Ereignisse finden Sie auf der Seite Aktivitäten.

Erläuterung präventiver Kontrollen

Eine präventive Kontrolle stellt sicher, dass die Konten Ihres Unternehmens Ihren Unternehmensrichtlinien entsprechen. Der Status einer präventiven Kontrolle ist entweder erzwungen oder nicht aktiviert. Eine präventive Kontrolle verhindert Richtlinienverstöße mithilfe von Service Control Policies (SCPs), Resource Control Policies (RCPs) oder deklarativen Richtlinien. Im Vergleich dazu informiert Sie eine detektive Kontrolle anhand definierter Regeln über verschiedene Ereignisse oder Zustände. AWS Config

Einige Ihrer Benutzer, z. B. AWS Entwickler, müssen möglicherweise wissen, welche präventiven Kontrollen für alle von ihnen verwendeten Konten und Organisationseinheiten gelten, damit sie technische Lösungen entwickeln können. Das folgende Verfahren bietet Unterstützung darin, wie diese Informationen gemäß den Informationsverwaltungsrichtlinien Ihrer Organisation für die richtigen Benutzer bereitgestellt werden.

> **Note**
>
> Bei diesem Verfahren wird davon ausgegangen, dass Sie bereits mindestens eine untergeordnete Organisationseinheit in Ihrer landing zone sowie mindestens einen AWS IAM Identity Center Benutzer erstellt haben.

Beispiel: Um präventive Kontrollen für Benutzer aufzuzeigen, die es wissen müssen

1. Melden Sie sich bei der AWS Control Tower Tower-Konsole unter an https://console.aws.amazon.com/controltower/.
2. Wählen Sie in der linken Navigationsleiste Organisation aus.
3. Wählen Sie aus der Tabelle den Namen einer der Organisationseinheiten aus, für die Ihr Benutzer Informationen zu den entsprechenden Kontrollen benötigt.
4. Notieren Sie sich den Namen der OU und die Steuerelemente, die für diese OU gelten.
5. Wiederholen Sie die beiden vorherigen Schritte für jede Organisationseinheit, über die der Benutzer Informationen benötigt.

Ausführliche Informationen zu den Kontrollen und ihren Funktionen finden Sie unter Über Kontrollen in AWS Control Tower.

Planen Sie Ihre AWS Control Tower Tower-Landezone

Wenn Sie den Einrichtungsprozess durchlaufen, startet AWS Control Tower eine wichtige Ressource, die mit Ihrem Konto verknüpft ist. Sie wird als landing zone bezeichnet und dient als Startseite für Ihre Organisationen und deren Konten.

> **Note**
>
> Sie können eine Landing Zone pro Organisation haben.

Informationen zu einigen bewährten Methoden, die Sie bei der Planung und Einrichtung Ihrer landing zone beachten sollten, finden Sie unterAWS Strategie für mehrere Konten für Ihre AWS Control Tower Tower-Landezone.

Möglichkeiten zur Einrichtung von AWS Control Tower

Sie können eine AWS Control Tower Tower-Landezone in einer bestehenden Organisation einrichten, oder Sie können damit beginnen, eine neue Organisation zu erstellen, die Ihre AWS Control Tower Tower-Landezone enthält.

- Starten Sie AWS Control Tower in einer bestehenden Organisation: Dieser Abschnitt richtet sich an Kunden, die bereits AWS Organizations bereit sind, die Steuerung durch AWS Control Tower in Angriff zu nehmen.
- Starten Sie AWS Control Tower in einer neuen Organisation: Dieser Abschnitt richtet sich an Kunden ohne bestehende AWS Organizations Organisationseinheiten und Konten.

> **Note**
>
> Wenn Sie bereits über eine AWS Organizations landing zone verfügen, können Sie die AWS Control Tower Governance von der bestehenden landing zone auf einige oder alle Ihrer vorhandenen Organisationseinheiten und Konten innerhalb einer Organisation ausdehnen. Weitere Informationen finden Sie unter Verwaltung vorhandener Organisationen und Konten.

Funktionen vergleichen

Im Folgenden finden Sie einen kurzen Vergleich der Unterschiede zwischen dem Hinzufügen von AWS Control Tower zu einer bestehenden Organisation oder der Ausweitung der AWS Control Tower Tower-Governance auf Organisationseinheiten und Konten. Außerdem gelten einige besondere Überlegungen, wenn Sie von der AWS Landing Zone-Lösung zu AWS Control Tower wechseln.

Informationen zum Hinzufügen zu einer bestehenden Organisation: Das Hinzufügen von AWS Control Tower zu einer bestehenden Organisation ist etwas, das Sie in der AWS Konsole erledigen können. In diesem Fall haben Sie bereits eine Organisation, die Sie im AWS Organizations Service erstellt haben, diese Organisation ist derzeit nicht bei AWS Control Tower registriert und Sie möchten anschließend eine landing zone hinzufügen.

Wenn Sie einer bestehenden Organisation eine landing zone hinzufügen, richtet AWS Control Tower auf dieser AWS Organizations Ebene eine parallel Struktur ein. Die Organisationseinheiten und Konten innerhalb Ihrer bestehenden Organisation werden dadurch nicht geändert.

Über Extending Governance: Die Erweiterung der Governance gilt für bestimmte Organisationseinheiten und Konten innerhalb einer einzelnen Organisation, die bereits bei AWS Control Tower registriert ist, was bedeutet, dass für diese Organisation bereits eine landing zone existiert. Die Ausweitung der Governance bedeutet, dass die Kontrollen von AWS Control Tower so erweitert werden, dass ihre Einschränkungen für die spezifischen Organisationseinheiten und Konten innerhalb dieser registrierten Organisation gelten. In diesem Fall starten Sie keine neue landing zone, sondern erweitern nur die aktuelle landing zone für Ihr Unternehmen.

> **Important**
>
> Besondere Überlegung: Wenn Sie derzeit die AWS Landing Zone-Lösung (ALZ) für verwenden AWS Organizations, wenden Sie sich an Ihren AWS Lösungsarchitekten, bevor Sie versuchen, AWS Control Tower in Ihrer Organisation zu aktivieren. AWS Control Tower kann keine Vorabprüfungen durchführen, um festzustellen, ob AWS Control Tower Ihre aktuelle Landezone-Bereitstellung beeinträchtigen könnte. Weitere Informationen finden Sie unter Exemplarische Vorgehensweise: Wechseln Sie von ALZ zum AWS Control Tower. Weitere Informationen zum Verschieben von Konten von einer landing zone in eine andere finden Sie unter Wenn das Konto die Voraussetzungen nicht erfüllt

Starten Sie AWS Control Tower in einer bestehenden Organisation

Durch die Einrichtung einer AWS Control Tower Tower-Landezone in einer bestehenden Organisation können Sie sofort mit der Arbeit beginnen, parallel zu Ihrer bestehenden AWS Organizations Umgebung. Ihre anderen innerhalb erstellten AWS Organizations Organisationseinheiten bleiben unverändert, da sie nicht bei AWS Control Tower registriert sind. Sie können diese OUs und Konten weiterhin genau so verwenden, wie sie sind.

AWS Control Tower konsolidiert, indem das Verwaltungskonto Ihrer bestehenden Organisation als Verwaltungskonto verwendet wird. Es ist kein neues Verwaltungskonto erforderlich. Sie können Ihre AWS Control Tower Tower-Landezone von Ihrem bestehenden Verwaltungskonto aus starten.

> **Note**
>
> Um AWS Control Tower in einer bestehenden Organisation einzurichten, müssen Ihre Service-Limits die Erstellung von mindestens zwei zusätzlichen Konten ermöglichen.

Auswirkungen der Erweiterung Ihrer bestehenden Organisation um AWS Control Tower

AWS Control Tower erstellt zwei Konten in Ihrer Organisation: ein Prüfkonto und ein Protokollkonto. Diese Konten zeichnen die von Ihrem Team ergriffenen Maßnahmen in ihren individuellen Endbenutzerkonten auf. Die Konten Audit und Log Archive werden in der Sicherheits-OU in Ihrer AWS Control Tower Tower-Landingzone angezeigt.

Wenn Sie Ihre landing zone einrichten, werden die von AWS Control Tower hinzugefügten Konten Teil Ihrer bestehenden AWS Organizations Konten und somit Teil der Abrechnung für Ihre bestehende Organisation.

Zusammenfassung der Funktionen

Die Aktivierung von AWS Control Tower in einer bestehenden AWS Organizations Organisation bietet mehrere wichtige Verbesserungen für die Organisation.

- Es ermöglicht eine einheitliche Abrechnung für alle Gruppen Ihrer Organisation, da die von AWS Control Tower hinzugefügten Konten Teil Ihrer bestehenden Organisation werden.
- Es gibt Ihnen die Möglichkeit, alle Konten von einem Verwaltungskonto in Ihrer Organisationseinheit aus zu verwalten.
- Es vereinfacht die Anwendung und Durchsetzung von Sicherheits- und Compliance-Kontrollen für bestehende und neue Konten.

> **Important**
>
> Wenn Sie Ihre AWS Control Tower-Landezone in einer bestehenden AWS Organizations Organisation einrichten, können Sie die AWS Control Tower Tower-Governance nicht von dieser Organisation auf andere Organisationseinheiten oder Konten ausdehnen, die nicht bei AWS Control Tower registriert sind.

Um AWS Control Tower in Ihrer bestehenden Organisation zu starten, folgen Sie dem unter beschriebenen VerfahrenErste Schritte mit AWS Control Tower.

Weitere Informationen darüber, wie AWS Control Tower mit bestehenden AWS Organizations Organisationen interagiert, finden Sie unterSteuern Sie Organisationen und Konten mit AWS Control Tower.

Starten Sie AWS Control Tower in einer neuen Organisation

Wenn Sie neu bei AWS Control Tower sind und noch nicht damit gearbeitet haben AWS Organizations, beginnen Sie am besten mit unserem Einrichtung Dokument.

AWS Control Tower richtet automatisch eine Organisation für Sie ein, wenn Sie noch keine eingerichtet haben.

AWS Strategie für mehrere Konten für Ihre AWS Control Tower Tower-Landezone

AWS Control Tower Tower-Kunden suchen häufig Unterstützung bei der Einrichtung ihrer AWS Umgebung und Konten, um optimale Ergebnisse zu erzielen.AWS hat eine Reihe einheitlicher Empfehlungen, die sogenannte Multi-Account-Strategie, erstellt, um Ihnen zu helfen, Ihre AWS Ressourcen, einschließlich Ihrer AWS Control Tower Tower-Landezone, optimal zu nutzen.

Im Wesentlichen fungiert AWS Control Tower als Orchestrierungsebene, die mit anderen AWS Services zusammenarbeitet, die Sie bei der Implementierung der AWS Multi-Account-Empfehlungen für AWS Konten und unterstützen. AWS Organizations Nachdem Ihre landing zone eingerichtet wurde, unterstützt Sie AWS Control Tower weiterhin bei der Einhaltung Ihrer Unternehmensrichtlinien und Sicherheitspraktiken für mehrere Konten und Workloads.

Die meisten Landezonen entwickeln sich im Laufe der Zeit. Wenn die Anzahl der Organisationseinheiten (OUs) und Konten in Ihrer AWS Control Tower Tower-Landezone zunimmt, können Sie Ihre AWS Control Tower Tower-Bereitstellung so erweitern, dass Ihre Workloads effektiv organisiert werden können. Dieses Kapitel enthält Anleitungen zur Planung und Einrichtung Ihrer AWS Control Tower Tower-Landing landing zone im Einklang mit der AWS Multi-Account-Strategie und deren Erweiterung im Laufe der Zeit.

Eine allgemeine Diskussion über bewährte Methoden für Organisationseinheiten finden Sie unter Bewährte Methoden für Organisationseinheiten mit. AWS Organizations

AWS Strategie für mehrere Konten: Leitfaden für bewährte Verfahren

AWS Bewährte Verfahren für eine gut strukturierte Umgebung empfehlen, dass Sie Ihre Ressourcen und Workloads auf mehrere Konten aufteilen. AWS Sie können sich AWS Konten als isolierte Ressourcencontainer vorstellen: Sie bieten eine Kategorisierung der Arbeitslast sowie eine Reduzierung des Explosionsradius, wenn etwas schief geht.

Definition eines Kontos AWS

Ein AWS Konto fungiert als Ressourcencontainer und Grenze zur Ressourcenisolierung.

> **Note**
>
> Ein AWS Konto ist nicht dasselbe wie ein Benutzerkonto, das über Federation oder AWS Identity and Access Management (IAM) eingerichtet wird.

Weitere Informationen zu Konten AWS

Ein AWS Konto bietet die Möglichkeit, Ressourcen zu isolieren und Sicherheitsbedrohungen für Ihre AWS Workloads einzudämmen. Ein Konto bietet auch einen Mechanismus für die Abrechnung und Verwaltung einer Workload-Umgebung.

Das AWS Konto ist der primäre Implementierungsmechanismus zur Bereitstellung eines Ressourcencontainers für Ihre Workloads. Wenn Ihre Umgebung gut strukturiert ist, können Sie mehrere AWS Konten effektiv verwalten und somit mehrere Workloads und Umgebungen verwalten.

AWS Control Tower richtet eine gut strukturierte Umgebung ein. Es stützt sich auf AWS Konten und unterstützt diese bei der Verwaltung von Änderungen an Ihrer Umgebung, die sich auf mehrere Konten erstrecken können. AWS Organizations

Definition einer gut strukturierten Umgebung

AWS definiert eine gut strukturierte Umgebung als eine Umgebung, die mit einer landing zone beginnt.

AWS Control Tower bietet eine landing zone, die automatisch eingerichtet wird. Es setzt Kontrollen durch, um die Einhaltung Ihrer Unternehmensrichtlinien für mehrere Konten in Ihrer Umgebung sicherzustellen.

Definition einer landing zone

Die landing zone ist eine Cloud-Umgebung, die einen empfohlenen Ausgangspunkt bietet, einschließlich Standardkonten, Kontostruktur, Netzwerk- und Sicherheitslayouts usw. Von einer landing zone aus können Sie Workloads bereitstellen, die Ihre Lösungen und Anwendungen nutzen.

Richtlinien für die Einrichtung einer gut strukturierten Umgebung

Die drei wichtigsten Komponenten einer gut strukturierten Umgebung, die in den folgenden Abschnitten erläutert werden, sind:

- Mehrere Konten AWS
- Mehrere Organisationseinheiten (OUs)
- Eine gut geplante Struktur

Verwenden Sie mehrere AWS-Konten

Ein Konto reicht nicht aus, um eine gut strukturierte Umgebung einzurichten. Durch die Verwendung mehrerer Konten können Sie Ihre Sicherheitsziele und Geschäftsprozesse optimal unterstützen. Hier sind einige Vorteile der Verwendung eines Ansatzes mit mehreren Konten:

- Sicherheitskontrollen — Anwendungen haben unterschiedliche Sicherheitsprofile und erfordern daher unterschiedliche Kontrollrichtlinien und -mechanismen. Zum Beispiel ist es viel einfacher, mit einem Wirtschaftsprüfer zu sprechen und auf ein einziges Konto hinzuweisen, das den Payment Card Industry (PCI) -Workload hostet.
- Isolierung — Ein Konto ist eine Sicherheitseinheit. Potenzielle Risiken und Sicherheitsbedrohungen können innerhalb eines Kontos eingedämmt werden, ohne dass sich dies auf andere auswirkt. Aus Sicherheitsgründen müssen Sie Konten daher möglicherweise voneinander isolieren. Beispielsweise können Sie Teams mit unterschiedlichen Sicherheitsprofilen haben.
- Viele Teams — Teams haben unterschiedliche Verantwortlichkeiten und Ressourcenanforderungen. Durch die Einrichtung mehrerer Konten können sich die Teams nicht gegenseitig stören, wie dies bei der Verwendung desselben Kontos der Fall wäre.
- Datenisolierung — Die Isolierung von Datenspeichern auf ein Konto trägt dazu bei, die Anzahl der Personen zu begrenzen, die Zugriff auf Daten haben und den Datenspeicher verwalten können. Diese Isolierung trägt dazu bei, die unbefugte Offenlegung hochvertraulicher Daten zu

verhindern. Beispielsweise trägt die Datenisolierung dazu bei, die Einhaltung der Allgemeinen Datenschutzverordnung (DSGVO) zu unterstützen.

- Geschäftsprozess — Geschäftsbereiche oder Produkte haben oft völlig unterschiedliche Zwecke und Prozesse. Individuelle Konten können eingerichtet werden, um geschäftsspezifischen Anforderungen gerecht zu werden.
- Abrechnung — Ein Konto ist die einzige Möglichkeit, Posten auf Abrechnungsebene zu trennen, einschließlich Dinge wie Überweisungsgebühren usw. Die Strategie für mehrere Konten hilft dabei, separate fakturierbare Posten für verschiedene Geschäftsbereiche, Funktionsteams oder einzelne Benutzer zu erstellen.
- Kontingentzuweisung — AWS Kontingente werden pro Konto eingerichtet. Durch die Aufteilung der Arbeitslasten auf verschiedene Konten erhält jedes Konto (z. B. ein Projekt) ein genau definiertes, individuelles Kontingent.

Verwenden Sie mehrere Organisationseinheiten

AWS Control Tower und andere Frameworks zur Kontoorchestrierung können Änderungen vornehmen, die Kontogrenzen überschreiten. Daher beziehen sich die AWS bewährten Methoden auf kontoübergreifende Änderungen, die möglicherweise eine Umgebung beschädigen oder ihre Sicherheit gefährden können. In einigen Fällen können sich Änderungen auf das gesamte Umfeld auswirken und nicht nur politische Maßnahmen betreffen. Daher empfehlen wir, dass Sie mindestens zwei obligatorische Konten einrichten: Production und Staging.

Darüber hinaus werden AWS Konten aus Gründen der Verwaltung und Kontrolle häufig in Organisationseinheiten (OUs) gruppiert. Organisationseinheiten sind darauf ausgelegt, die Durchsetzung von Richtlinien über mehrere Konten hinweg zu gewährleisten.

Wir empfehlen, dass Sie mindestens eine Vorproduktions- (oder Staging-) Umgebung einrichten, die sich von Ihrer Produktionsumgebung unterscheidet — mit unterschiedlichen Kontrollen und Richtlinien. Die Produktions- und Staging-Umgebungen können als separate Organisationseinheiten erstellt und verwaltet und als separate Konten abgerechnet werden. Darüber hinaus möchten Sie möglicherweise eine Sandbox-Organisationseinheit für Codetests einrichten.

Verwenden Sie eine gut geplante Struktur für OUs in Ihrer landing zone

AWS Control Tower richtet einige OUs automatisch für Sie ein. Wenn Ihre Workloads und Anforderungen im Laufe der Zeit zunehmen, können Sie die ursprüngliche Landezone-Konfiguration an Ihre Bedürfnisse anpassen.

> **Note**
>
> Die in den Beispielen angegebenen Namen entsprechen den vorgeschlagenen AWS Benennungskonventionen für die Einrichtung einer Umgebung mit mehreren Konten AWS . Sie können Ihre Organisationseinheiten umbenennen, nachdem Sie Ihre landing zone eingerichtet haben, indem Sie auf der OU-Detailseite auf Bearbeiten klicken.

Empfehlungen

Nachdem AWS Control Tower die erste, erforderliche Organisationseinheit für Sie eingerichtet hat — die Sicherheits-OU — empfehlen wir, einige zusätzliche Organisationseinheiten in Ihrer landing zone zu erstellen.

Wir empfehlen, dass Sie AWS Control Tower erlauben, mindestens eine zusätzliche Organisationseinheit, die sogenannte Sandbox-Organisationseinheit, zu erstellen. Diese OU ist für Ihre Softwareentwicklungsumgebungen vorgesehen. AWS Control Tower kann die Sandbox-Organisationseinheit bei der Erstellung der landing zone für Sie einrichten, sofern Sie sie auswählen.

Zwei empfohlene weitere Organisationseinheiten, die Sie selbst einrichten können: die Infrastruktur-OU, die Ihre Shared Services und Netzwerkkonten enthält, und eine OU zur Speicherung Ihrer Produktionsworkloads, die sogenannte Workloads-OU. Sie können zusätzliche Organisationseinheiten in Ihrer landing zone über die AWS Control Tower Tower-Konsole auf der Seite Organisationseinheiten hinzufügen.

Neben den automatisch eingerichteten Organisationseinheiten werden auch empfohlene Organisationseinheiten empfohlen

- Infrastruktur-OU — Enthält Ihre Shared Services und Netzwerkkonten.

  > **Note**
  >
  > AWS Control Tower richtet die Infrastruktur-OU nicht für Sie ein.

- Sandbox OU — Eine OU für Softwareentwicklung. Beispielsweise kann es ein festes Ausgabenlimit haben oder es ist möglicherweise nicht mit dem Produktionsnetzwerk verbunden.

> **Note**
>
> AWS Control Tower empfiehlt, die Sandbox-Organisationseinheit einzurichten, dies ist jedoch optional. Es kann im Rahmen der Konfiguration Ihrer landing zone automatisch eingerichtet werden.

- Workloads OU — Enthält Konten, die Ihre Workloads ausführen.

> **Note**
>
> AWS Control Tower richtet die Workloads OU nicht für Sie ein.

Weitere Informationen finden Sie unter So richtet AWS Control Tower Ihre Umgebung mit mehreren Konten ein.

Passen Sie Ihre OU-Struktur an AWS Strategie für mehrere Konten

AWS Control Tower unterstützt eine verschachtelte OU-Hierarchie, was bedeutet, dass Sie eine hierarchische OU-Struktur erstellen können, die den Anforderungen Ihrer Organisation entspricht. Sie können eine AWS Control Tower Tower-Umgebung einrichten, die den strategischen Leitlinien für AWS mehrere Konten entspricht.

Weitere Informationen zur Funktionsweise von AWS Control Tower mit verschachtelten OU-Strukturen finden Sie unterVerschachtelte Organisationseinheiten im AWS Control Tower.

Informationen zu empfohlenen Organisationseinheiten und Konten, die über die von AWS Control Tower standardmäßig eingerichteten hinausgehen, finden Sie im AWS Whitepaper unter Empfohlene Organisationseinheiten und Konten.

Über den Root

The Root ist keine Organisationseinheit. Es ist ein Container für das Verwaltungskonto und für alle Organisationseinheiten und Konten in Ihrer Organisation. Konzeptionell gesehen enthält das Stammverzeichnis alle Organisationseinheiten. Es kann nicht gelöscht werden. Sie können registrierte Konten nicht auf Root-Ebene innerhalb von AWS Control Tower verwalten. Steuern Sie stattdessen registrierte Konten innerhalb Ihrer Organisationseinheiten. Ein hilfreiches Diagramm finden Sie in der AWS Organizations Dokumentation.

Administrative Tipps für die Einrichtung der landing zone

Hier finden Sie einige Tipps zur Einrichtung und Konfiguration Ihrer landing zone.

- Die AWS Region, in der Sie am meisten arbeiten, sollte Ihre Heimatregion sein.
- Richten Sie Ihre landing zone ein und stellen Sie Ihre Account Factory Factory-Konten von Ihrer Heimatregion aus bereit.
- Wenn Sie in mehrere AWS Regionen investieren, stellen Sie sicher, dass sich Ihre Cloud-Ressourcen in der Region befinden, in der Sie den Großteil Ihrer Cloud-Verwaltungsarbeit erledigen und Ihre Workloads ausführen werden.
- Indem Sie Ihre Workloads und Logs in derselben AWS Region speichern, reduzieren Sie die Kosten, die mit dem Verschieben und Abrufen von Protokollinformationen zwischen Regionen verbunden wären.
- Das Audit und andere Amazon S3 S3-Buckets werden in derselben AWS Region erstellt, von der aus Sie AWS Control Tower starten. Wir empfehlen, diese Buckets nicht zu verschieben.
- Sie können Ihre eigenen Log-Buckets im Log Archive-Konto erstellen, dies wird jedoch nicht empfohlen. Achten Sie darauf, die von AWS Control Tower erstellten Buckets zu belassen.
- Ihre Amazon S3 S3-Zugriffsprotokolle müssen sich in derselben AWS Region wie die Quell-Buckets befinden.
- Beim Start müssen AWS Security Token Service (STS) -Endpunkte im Verwaltungskonto für alle von AWS Control Tower unterstützten Regionen aktiviert werden. Andernfalls kann der Start während des Konfigurationsprozesses fehlschlagen.
- AWS Control Tower unterstützt Tagging nur für aktivierte Kontrollen. Weitere Informationen finden Sie unter APIs für das Taggen von AWS Control Tower Control.
- Wir empfehlen, die Multi-Faktor-Authentifizierung (MFA) für jedes Konto zu aktivieren, das AWS Control Tower verwaltet.
- Alternativ können Sie die AWS Root-Zugriffsverwaltungsfunktion verwenden, mit der Root-Aktionen für Mitgliedskonten ausgeführt werden können und die Notwendigkeit entfällt, MFA für jedes Konto zu aktivieren. Weitere Informationen finden Sie unter Zentrale Verwaltung des Root-Zugriffs für Kunden, die AWS Organizations

Überlegungen zu VPCs

- Die von AWS Control Tower erstellte VPC ist auf das beschränkt, AWS-Regionen in dem AWS Control Tower verfügbar ist. Einige Kunden, deren Workloads in nicht unterstützten Regionen

ausgeführt werden, möchten möglicherweise die VPC deaktivieren, die mit Ihrem Account Factory erstellt wurde. Möglicherweise ziehen sie es vor, mithilfe des Service Catalog-Portfolios eine neue VPC zu erstellen oder eine benutzerdefinierte VPC zu erstellen, die nur in den erforderlichen Regionen ausgeführt wird.

- Die von AWS Control Tower erstellte VPC entspricht nicht der Standard-VPC, die für alle erstellt wurde. AWS-Konten In Regionen, in denen AWS Control Tower unterstützt wird, löscht AWS Control Tower die Standard-VPC, wenn die AWS Control Tower Tower-VPC erstellt wird.
- Wenn Sie Ihre Standard-VPC in Ihrer AWS Heimatregion löschen, löschen Sie sie am besten in allen anderen AWS Regionen.

Leitfaden zur Migration von Landing Zone v4.0

AWS Control Tower landing zone 4.0 führt eine umfassende Überarbeitung der Landing Zone-Architektur ein und bietet ein flexibles, dediziertes Steuerungserlebnis und vollständig optionale Serviceintegrationen. Zu den wichtigsten Verbesserungen gehört die Möglichkeit AWS Config, AWS CloudTrail und AWS Backup Integrationen selektiv zu aktivieren, mit speziellen Ressourcen für AWS Config und AWS CloudTrail für eine verbesserte Isolierung. SecurityRoles

Mit der Version werden die verbindlichen Anforderungen an die Organisationsstruktur gestrichen, sodass Kunden ihre eigenen Anforderungen definieren können. Gleichzeitig wird ein neuer Support `ConfigBaseline` für detektive Kontrollen eingeführt, ohne dass umfassende Anforderungen erforderlich sind. `AWSControlTowerBaseline` Ein serviceverknüpfter Config Aggregator ersetzt frühere Aggregationsmethoden und optimiert die Erfassung von Compliance-Daten.

Darüber hinaus wird das Manifestfeld optional, was minimalistische Landezone-Bereitstellungen ermöglicht, die sich ausschließlich auf AWS Organizations Integration und Steuerung konzentrieren. Diese Änderungen bieten mehr Anpassungsmöglichkeiten bei gleichzeitiger Beibehaltung robuster Governance-Funktionen, sodass Kunden AWS Control Tower effektiver an ihre spezifischen Bedürfnisse anpassen können.

Themen

- Die wichtigsten Änderungen
- Aktualisierungen der AWS Config
- Vergleich der Funktionen mit und ohne AWS Config Integration

Die wichtigsten Änderungen

Note

- Die Definitionen von „registriert“ und „registriert“ haben sich mit dieser neuen Version von AWS Control Tower geändert. Wenn auf Ihrem account/OU System eine AWS Control Tower Tower-Ressource aktiviert ist (z. B. Control oder Baseline), wird diese als verwaltete Ressource betrachtet. Die Definition wird nicht mehr vom Vorhandensein der `AWSControlTowerBaseline` Baseline abhängen.
- Service-Linked Rollen bleiben in allen landing zone Zone-Versionen erhalten und werden nicht mehr gelöscht, wenn die Registrierung von Organisationseinheiten aufgehoben wird.
- Service-Linked Rollen können von Kunden nach der Außerbetriebnahme der landing zone nur manuell gelöscht werden

Aktualisierung von Version 3.3 oder früher auf Version 4.0

Deaktivieren Sie die Dienstintegrationen (AWS Config, SecurityRoles) nicht als Teil des Versionsupgrades. In landing zone Zone-Versionen 3.3 und früher SecurityRoles waren sie immer implizit aktiviert. AWS Config Version 4.0 stellt diese Integrationen zum ersten Mal als konfigurierbare Optionen zur Verfügung. Nach dem erfolgreichen Upgrade auf Version 4.0 können Sie die Serviceintegrationen nach Bedarf deaktivieren.

- Pre-requisite für Landing Zone 4.0: Stellen Sie beim Upgrade auf Version 4.0 über die API sicher, dass die `AWSControlTowerCloudTrailRole` Servicerolle die neue verwaltete Richtlinie `AWSControlTowerCloudTrailRolePolicy` anstelle der vorhandenen Inline-Richtlinie verwendet. Trennen Sie die aktuelle Inline-Richtlinie und hängen Sie die neue verwaltete Richtlinie an, wie in der Dokumentation beschrieben.
- Optionales Manifest: Das Manifestfeld in der Landingzone-API ist jetzt optional. Kunden können Landing Zones ohne Serviceintegrationen erstellen. Für Bestandskunden, die das Manifestfeld bereits verwenden, hat dies keine Auswirkungen.
- Optionale Organisationsstruktur: AWS Control Tower erzwingt oder verwaltet die Erstellung der Sicherheits-OU nicht mehr, sodass Kunden ihre eigene Organisationsstruktur definieren und verwalten können. AWS Control Tower verlangt jedoch, dass alle Konten, die für jede AWS-Serviceintegration konfiguriert sind, derselben übergeordneten Organisationseinheit angehören.

Für Kunden, die den AWS Control Tower bereits eingerichtet haben und über die Security OU verfügen, hat dies keine Auswirkungen. AWS Control Tower stellt automatisch die Ressourcen und Kontrollen bereit, die für die Verwaltung der Service-Integrationskonten in der Security OU erforderlich sind. Wenn beispielsweise die AWS Config-Integration aktiviert ist, ist die AWS Config-Aufzeichnung in allen Serviceintegrationskonten aktiviert. Die AWS Control Tower Baseline und die AWS Config Baseline gelten nicht für die Security OU und die Service-Integrationskonten. Um die Serviceintegrationen zu ändern, aktualisieren Sie die landing zone Zone-Einstellungen.

> **Note**
>
> - Die Einrichtung der Organisationsstruktur für die AWS Control Tower landing zone 4.0 hat sich gegenüber früheren landing zone Zone-Versionen geändert. AWS Control Tower erstellt die angegebene Sicherheits-OU nicht mehr. Die OU mit den Service-Integrationskonten wird die designierte Sicherheits-OU sein.
> - Wenn Mitgliedskonten in die Organisationseinheit verschoben werden, in der sich die Konten für jede Integration befinden, werden die aktivierten Steuerelemente für diese Organisationseinheit unabhängig davon, ob die automatische Registrierung aktiviert oder deaktiviert ist, verschoben.

Basisstatus für die Sicherheits-OU: Die AWS Control Tower Baseline und die AWS Config Baseline können nicht auf die Sicherheits-OU angewendet werden. Die Sicherheits-OU zeigt für diese Baselines den Basisstatus „Nicht zutreffend“ an. Dieser Status wird erwartet. Der BackupBaseline kann auf die Sicherheits-OU angewendet werden.

AWS Control Tower verwaltet Service-Integrationskonten über die landing zone, nicht über OU-level Baselines. Wenn ein Service-Integration-Konto den Basisstatus „Nicht aktiviert“ anzeigt und die zugehörige Service-Integration deaktiviert ist, verwaltet AWS Control Tower dieses Konto nicht mehr.

Konten in der Sicherheits-OU, die nicht als Serviceintegrationskonten ausgewiesen sind, erhalten keine Basisressourcen. Um diese Konten zu verwalten, verschieben Sie sie in eine verwaltete Organisationseinheit und erweitern Sie die Verwaltung.

IAM Identity Center-Berechtigungssätze für Serviceintegrationskonten: AWS Control Tower stellt IAM Identity Center-Berechtigungssätze für das Logging-Konto und das SecurityRoles Konto bereit. AWS Control Tower stellt keine Berechtigungssätze für das Config-Konto oder das Backup-Konto bereit. Um über IAM Identity Center auf das Config- oder Backup-Konto zuzugreifen, erstellen Sie

Berechtigungssätze manuell mithilfe der IAM Identity Center-Ressourcen, die AWS Control Tower bereitgestellt hat.

- Drift-Benachrichtigungen: AWS Control Tower beendet das Senden von Drift-Benachrichtigungen an das SNS-Thema für alle Kunden in der landing zone 4.0 und höher und beginnt stattdessen, Drift-Benachrichtigungen EventBridge an das Verwaltungskonto zu senden. Um diese Benachrichtigungen zu erhalten, erstellen Sie eine EventBridge Regel im Verwaltungskonto. Konfigurieren Sie dann ein Ziel, z. B. ein SNS-Thema oder eine Lambda-Funktion. Weitere Informationen zu Drift-Benachrichtigungen und EventBridge Beispielereignissen finden Sie unter Arten von Abweichungen in der Unternehmensführung.
- Optionale Serviceintegrationen: Sie haben jetzt die Möglichkeit, enable/disable alle AWS Control Tower Tower-Integrationen AWS Config, einschließlich AWS, und, zu CloudTrail nutzen SecurityRoles. AWS Backup Diese Integrationen verfügen jetzt auch über erforderliche `enabled` Flags in der API. Die Baselines, die möglicherweise für Ihre landing zone oder Ihre gemeinsamen Konten gelten, hängen jetzt voneinander ab. Die spezifischen Abhängigkeiten der Integrationen sind:
  - Aktivierung:
    - `CentralSecurityRolesBaseline`→ muss aktiviert `CentralConfigBaseline` sein
    - `IdentityCenterBaseline`→ `CentralSecurityRolesBaseline` muss aktiviert sein
    - `BackupCentralVaultBaseline`→ `CentralSecurityRolesBaseline` muss aktiviert sein
    - `BackupAdminBaseline`→ `CentralSecurityRolesBaseline` muss aktiviert sein
    - `LogArchiveBaseline`→ unabhängig (keine Abhängigkeiten)
    - `CentralConfigBaseline`→ unabhängig (keine Abhängigkeiten)
  - Behinderung:
    - `CentralConfigBaseline`kann nur deaktiviert werden`CentralSecurityRolesBaseline`, wenn`IdentityCenterBaseline`, `BackupAdminBaseline` und `BackupCentralVaultBaseline` Baselines zuerst deaktiviert wurden.
    - `CentralSecurityRolesBaseline`kann nur deaktiviert werden`IdentityCenterBaseline`, wenn `BackupAdminBaseline` und `BackupCentralVaultBaseline` Baselines zuerst deaktiviert werden.
    - `IdentityCenterBaseline`kann unabhängig deaktiviert werden.
    - `BackupAdminBaseline`und `BackupCentralVaultBaseline` Baselines können unabhängig voneinander deaktiviert werden
    - `LogArchiveBaseline`können unabhängig deaktiviert werden

⚠ Umfang von AWS Config Aktivierung der Serviceintegration

Durch die Aktivierung der AWS Config Serviceintegration auf Landingzone-Ebene werden Config-Aufzeichnungsressourcen nur für Serviceintegrationskonten bereitgestellt. Um AWS Config Ressourcen (Config Recorder, Delivery Channel) für Mitgliedskonten bereitzustellen, aktivieren Sie die AWS Config Baseline für jede verwaltete Organisationseinheit einzeln.
Die Aktivierung der Config-Integration auf Landingzone-Ebene ist eine Voraussetzung für die Aktivierung der Config-Baseline auf OUs. Die Einstellung auf Landezonenebene allein stellt keine Config-Ressourcen für Mitgliedskonten bereit.
Weitere Informationen finden Sie unter Aktualisierungen der AWS Config.

⚠ CentralizedLogging Verhaltensänderung in Version 4.0

In landing zone Zone-Versionen 3.3 und früher wurde durch die CentralizedLogging Deaktivierung die Organisation CloudTrail ausgeschaltet und alle bereitgestellten Ressourcen wurden beibehalten. In Version 4.0 werden durch die CentralizedLogging Deaktivierung alle zugehörigen Ressourcen aus dem Protokollierungskonto gelöscht. Zu diesen Ressourcen gehören Config Recorder, Delivery Channel und CloudTrail-related Stack-Instances. Nach der Deaktivierung verwaltet AWS Control Tower das Logging-Konto nicht mehr.
Um die Verwaltung des Protokollierungskontos wiederherzustellen, aktivieren Sie das Konto erneut CentralizedLogging oder verschieben Sie es in eine verwaltete Organisationseinheit und erweitern Sie die Verwaltung.

Aktualisierungen der AWS Config

- Dedizierte Ressourcen für AWS Config und AWS CloudTrail: AWS Config und AWS verwenden CloudTrail jetzt separate dedizierte S3-Buckets und SNS-Themen anstelle von gemeinsam genutzten Ressourcen. Kunden haben nur begrenzte Flexibilität, ein einzelnes oder separate Konten für mehrere Integrationen zu verwenden.
  - Beim Upgrade auf AWS Control Tower landing zone Version 4.0 werden vorhandene Daten und S3-Buckets nicht verschoben. Die CloudTrail AWS-Integration verwendet weiterhin den vorhandenen S3-Bucket mit Präfix`aws-controltower-logs`. Die neuen AWS Config-

Daten nach dem Aktualisierungsvorgang werden in einem neuen S3-Bucket mit einem Präfix gespeichert`aws-controltower-config`, das AWS Control Tower in dem dafür vorgesehenen Konto erstellt CentralConfigBaseline.

> **Note**
>
> Wenn Sie die CloudTrail AWS-Integration in der landing zone 4.0 zum ersten Mal aktivieren, werden jedes Mal neue S3-Buckets mit Präfix erstellt `aws-controltower-cloudtrail`

- Änderungen des Datenstandorts: Bestandskunden, die von zuvor gemeinsam genutzten Ressourcen auf dedizierte Ressourcen umsteigen, verfügen über AWS Config CloudTrail AWS-Daten in verschiedenen S3-Buckets. Etablierte Kundenabläufe und Tools müssen möglicherweise aktualisiert werden, um auf Daten von neuen Bucket-Standorten aus zugreifen zu können.
- AWS CloudTrail bleibt weiterhin im selben bestehenden Bucket, aber die AWS Config Daten werden in einem neuen S3-Bucket gespeichert, der von AWS Control Tower erstellt wurde.
- Kunden können eine Bucket-übergreifende Replikation einrichten, wenn sie verschiedene Protokolle in einem einzigen Bucket zentralisieren möchten. Weitere Informationen finden Sie in der S3-Dokumentation.
- Wenn Sie Konten mit bereits vorhandenen AWS Config-Lieferkanälen registriert haben, die nicht von AWS Control Tower in Regionen erstellt wurden, die von AWS Control Tower verwaltet werden, aktualisieren Sie den S3-Bucket-Namen der Delivery Channels auf den neuen S3-Bucket mit Präfix `aws-controltower-config-logs-` im AWS Config-Integrationskonto, damit er mit den AWS Control Tower Tower-Konfigurationen in der landing zone 4.0 konsistent ist. Weitere Details finden Sie unter Konten registrieren, die bereits vorhanden sind AWS Config Ressourcen.

- AWS Config Integration auf landing zone Version 4.0: Bei der Migration zur landing zone 4.0 mit aktivierter AWS Config Integration würden Kunden die folgenden Änderungen sehen -

  1. Das bestehende Audit-Konto ist als delegierter Administrator für registriert. AWS Config
  2. Service-Linked Config Aggregator wird im Audit-Konto bereitgestellt (AWS Config zentrales Aggregatorkonto für Neukunden und Audit-Konto für Bestandskunden). Der neue Aggregator kann Daten von jedem AWS Config Recorder in der Organisation aggregieren, auch von Konten, die nicht von Control Tower verwaltet werden.

3. Bestehende Aggregatoren werden gelöscht — Der Organisationsaggregator im Verwaltungskonto (`aws-controltower-ConfigAggregatorForOrganizations`) und der Kontoaggregator im Auditkonto (`aws-controltower-GuardRailsComplianceAggregator`) werden gelöscht.
4. Da der Konfigurationsaggregator dienstgebunden ist, werden die Kontrollen, die mit gelöschten Aggregatoren verknüpft sind, automatisch entfernt.
   a. Änderungen an Tags verbieten, die von AWS Control Tower für AWS-Konfigurationsressourcen erstellt wurden
   b. Löschen von AWS Config Aggregation-Autorisierungen verbieten, die von AWS Control Tower erstellt wurden

- Neue **`ConfigBaseline`** Ausgangsbasis: Auf OU-Ebene gibt es jetzt eine separate Lösung `ConfigBaseline` für die Unterstützung von Detective Controls, ohne dass ein umfassender Support erforderlich ist. `AWSControlTowerBaseline` Weitere Informationen finden Sie in der Liste der Basistypen auf OU-Ebene. Für Bestandskunden, die die Standard-Landezone verwenden, sind alle Serviceintegrationen jetzt optional, mit dem Vorbehalt der Abhängigkeitsanforderungen, die unter beschrieben werden. Die wichtigsten Änderungen
- Service-Linked Config Aggregator: Ersetzt Organisations- und Kontoaggregatoren im AWS Config zentralen Aggregatorkonto.
  - Beim Upgrade auf landing zone 4.0 mit aktivierter AWS Config Integration benötigen Kunden `organizations:ListDelegatedAdministrators` Berechtigungen

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
           "backup:UpdateGlobalSettings",
           "controltower:CreateLandingZone",
           "controltower:UpdateLandingZone",
           "controltower:ResetLandingZone",
           "controltower:DeleteLandingZone",
           "controltower:GetLandingZoneOperation",
           "controltower:GetLandingZone",
           "controltower:ListLandingZones",
           "controltower:ListLandingZoneOperations",
           "controltower:ListTagsForResource",
```

```
            "controltower:TagResource",
            "controltower:UntagResource",
             "servicecatalog:*",
             "organizations:*",
             "organizations:RegisterDelegatedAdministrator",
             "organizations:EnableAWSServiceAccess",
             "organizations:DeregisterDelegatedAdministrator",
             "organizations:ListDelegatedAdministrators",
             "sso:*",
             "sso-directory:*",
             "logs:*",
             "cloudformation:*",
             "kms:*",
             "iam:GetRole",
             "iam:CreateRole",
             "iam:GetSAMLProvider",
             "iam:CreateSAMLProvider",
             "iam:CreateServiceLinkedRole",
             "iam:ListRolePolicies",
             "iam:PutRolePolicy",
             "iam:ListAttachedRolePolicies",
             "iam:AttachRolePolicy",
             "iam:DeleteRole",
             "iam:DeleteRolePolicy",
             "iam:DetachRolePolicy"
         ],
         "Resource": "*"
      }
   ]
}
```

Important

Nachdem Sie auf landing zone Version 4.0 aktualisiert und die AWS Config Integration aktiviert haben, müssen Sie den Aktivierungsprozess abschließen. Aktualisieren oder aktivieren Sie die `ConfigBaseline` auf allen Organisationseinheiten, in denen Sie Ressourcen bereitstellen AWS Config möchten. Solange Sie diesen Vorgang nicht abgeschlossen haben, empfängt Ihr AWS Config Aggregator keine Daten von Rekordern. Jedes Konto zeichnet weiterhin Daten auf und speichert sie. Nachdem Sie die Aktualisierung

von abgeschlossen haben`ConfigBaseline`, werden die aufgezeichneten Daten automatisch wieder im Aggregator gespeichert.
Wir empfehlen, dass Sie Ihre OUs `ConfigBaseline` so bald wie möglich nach der Aktivierung der Integration erneut registrieren oder aktivieren. AWS Config Durch das landing zone Zone-Update werden AWS Config Lieferberechtigungen aus der vorherigen S3-Bucket-Richtlinie entfernt, aber die Lieferkanäle werden erst nach Abschluss der Neuregistrierung auf den neuen Bucket umgeleitet. Bis dahin werden Konfigurationsschnappschüsse und der Konfigurationsverlauf nicht an S3 übermittelt.
Wenn sich die erneute Registrierung verzögert, werden einige dieser Daten nach Abschluss der erneuten Registrierung möglicherweise nicht an S3 übermittelt. Sie können alle Daten, die innerhalb Ihrer konfigurierten Aufbewahrungsfrist aufgezeichnet wurden, mithilfe der `config:GetResourceConfigHistory` API abrufen.

Vergleich der Funktionen mit und ohne AWS Config Integration

Mit Landing Zone 4.0 können Sie die AWS Config Integration deaktivieren. In der folgenden Tabelle sind die AWS Control Tower Tower-Funktionen zusammengefasst, die mit und ohne aktivierte AWS Config Integration in der landing zone verfügbar sind.

Features	AWS Config Integration aktiviert	AWS Config Integration deaktiviert
Präventive Kontrollen	✓	✓
Proaktive Kontrollen	✓	✓
Die Steuerung „Region Deny“ wurde auf Organisationseinheiten angewendet	✓	✓
Die Steuerung „Region Deny“ wurde auf die landing zone angewendet	✓	
Detektivische Kontrollen	✓	
Account Factory	✓	Alternative ansehen
Account Factory für Terraform (AFT)	✓	

Features	AWS Config Integration aktiviert	AWS Config Integration deaktiviert
Account Factory Anpassungen (AFC)	✓	
Integration von AWS Service Catalog mit Account Factory	✓	
Anpassungen für AWS Control Tower (cFCT)	✓	
Auf Organisationseinheiten angewendete Baselines	✓	
CloudTrail AWS-Integration und Baselines	✓	✓
AWS-Backup-Integration und Baselines	✓	
AWS IAM Identity Center-Integration und Baselines	✓	
AWS-SNS-Integration für Drift-Benachrichtigungen	✓	
EventBridge Amazon-Integration für Drift-Benachrichtigungen	✓	✓
Registrieren Sie OU	✓	Alternative ansehen

Alternativen

Account Factory

Wenn Sie die AWS Config Integration deaktiviert haben, können Sie die automatische Registrierung aktivieren und AWS Organizations zum Erstellen und Verschieben von Konten verwenden. Die Konten erben die Kontrollen, die auf die übergeordnete Organisationseinheit angewendet wurden.

Organisationseinheit registrieren

Wenn Sie die AWS Config Integration deaktiviert haben, können Sie sie AWS Organizations zum Erstellen von Organisationseinheiten verwenden. Aktivieren Sie dann die Kontrollen über die

Kontrollkatalogseite in der AWS Control Tower Tower-Konsole, setzen Sie die Kontrollen auf der Organisationsseite zurück oder verwenden Sie AWS Control Tower Tower-APIs.

Empfehlungen für die Einrichtung von Gruppen, Rollen und Richtlinien

Wenn Sie Ihre Landing Zone einrichten, sollten Sie im Voraus entscheiden, welche Benutzer Zugriff auf bestimmte Konten benötigen und warum. Ein Sicherheitskonto sollte beispielsweise nur für das Sicherheitsteam zugänglich sein, das Verwaltungskonto sollte nur für das Cloud-Administratorteam zugänglich sein usw.

Weitere Informationen zu diesem Thema finden Sie unter. Identitäts- und Zugriffsmanagement im AWS Control Tower

Empfohlene Einschränkungen

Sie können den Umfang des Administratorzugriffs auf Ihre Organisationen einschränken, indem Sie eine IAM-Rolle oder -Richtlinie einrichten, die es Administratoren ermöglicht, nur AWS Control Tower Tower-Aktionen zu verwalten. Der empfohlene Ansatz besteht darin, die IAM-Richtlinie zu verwenden. `arn:aws:iam::aws:policy/service-role/AWSControlTowerServiceRolePolicy` Wenn die `AWSControlTowerServiceRolePolicy` Rolle aktiviert ist, kann ein Administrator nur AWS Control Tower verwalten. Stellen Sie sicher, dass Sie in jedem Konto den entsprechenden Zugriff auf AWS Organizations für die Verwaltung Ihrer präventiven Kontrollen und SCPs sowie den AWS Config Zugriff auf für die Verwaltung detektiver Kontrollen angeben.

Wenn Sie das freigegebene Auditkonto in Ihrer Landing Zone einrichten, empfehlen wir, die `AWSSecurityAuditors`-Gruppe allen externen Auditoren Ihrer Konten zuzuweisen. Diese Gruppe erteilt ihren Mitgliedern eine schreibgeschützte Berechtigung. Ein Konto darf keine Schreibberechtigungen für die Umgebung haben, die von ihm überwacht wird, da dies gegen die Einhaltung der Anforderungen der Aufgabentrennung für Prüfer verstoßen kann.

Sie können in Ihren Richtlinien zur Rollenvertrauensstellung Bedingungen festlegen, um die Konten und Ressourcen einzuschränken, die mit bestimmten Rollen in AWS Control Tower interagieren. Wir empfehlen dringend, den Zugriff auf die `AWSControlTowerAdmin` Rolle einzuschränken, da dies weitreichende Zugriffsberechtigungen ermöglicht. Weitere Informationen finden Sie unter Optionale Bedingungen für Ihre Rollenvertrauensbeziehungen.

Anleitung zur Erstellung und Änderung von AWS Control Tower Tower-Ressourcen

Wir empfehlen die folgenden bewährten Methoden, wenn Sie Ressourcen in AWS Control Tower erstellen und ändern. Diese Anleitungen wird gegebenenfalls geändert, um Aktualisierungen am Service widerzuspiegeln. Denken Sie daran, dass das Modell der gemeinsamen Verantwortung für Ihre AWS Control Tower Tower-Umgebung gilt.

Allgemeine Anleitung

- Ändern oder löschen Sie keine Ressourcen, die von AWS Control Tower erstellt wurden, einschließlich Ressourcen im Verwaltungskonto, in den gemeinsamen Konten und in Mitgliedskonten. Wenn Sie diese Ressourcen ändern, müssen Sie möglicherweise Ihre landing zone aktualisieren oder eine Organisationseinheit erneut registrieren, und eine Änderung kann zu ungenauen Compliance-Berichten führen.

  Insbesondere:

  - Behalte einen aktiven AWS Config Rekorder. Wenn Sie Ihren Config-Recorder löschen, kann Detective Controls Abweichungen nicht erkennen und melden. Non-compliant Ressourcen werden möglicherweise aufgrund unzureichender Informationen als konform gemeldet.
  - Ändern oder löschen Sie nicht die AWS Identity and Access Management (IAM-) Rollen, die innerhalb der gemeinsamen Konten in der Sicherheits-Organisationseinheit (OU) erstellt wurden. Eine Änderung dieser Rollen kann ein Update der Landing Zone erforderlich machen.
  - Löschen Sie die `AWSControlTowerExecution` Rolle nicht aus Ihren Mitgliedskonten, auch nicht aus Konten, die nicht registriert sind. Wenn Sie dies tun, können Sie diese Konten nicht bei AWS Control Tower registrieren oder ihre unmittelbar übergeordneten Organisationseinheiten registrieren.
- Untersagen Sie nicht, dass diese AWS-Regionen über SCPs oder AWS -Security-Token-Service () verwendet werden.AWS STS Dies führt dazu, dass AWS Control Tower in einen undefinierten Zustand übergeht. Wenn Sie Regionen mit nicht zulassen AWS STS, schlägt Ihre Funktionalität in diesen Regionen fehl, da die Authentifizierung in diesen Regionen nicht verfügbar wäre. Verlassen Sie sich stattdessen auf die Funktion „Region verweigern“ von AWS Control Tower, wie in der Steuerung „Zugriff verweigern auf AWS Basis der Anfrage“ gezeigt AWS-Region, die auf der Ebene der landing zone funktioniert, oder die Kontrolle „Region verweigern“, die auf die Organisationseinheit angewendet wird und auf OU-Ebene arbeitet, um den Zugriff auf Regionen zu beschränken.

- Das AWS Organizations `FullAWSAccess` SCP muss angewendet werden und sollte nicht mit anderen SCPs zusammengeführt werden. Änderungen an diesem SCP werden nicht als Abweichung gemeldet. Einige Änderungen können jedoch die Funktionalität von AWS Control Tower auf unvorhersehbare Weise beeinträchtigen, wenn der Zugriff auf bestimmte Ressourcen verweigert wird. Wenn der SCP beispielsweise getrennt oder geändert wird, kann ein Konto den Zugriff auf einen AWS Config Rekorder verlieren oder eine Lücke in CloudTrail der Protokollierung entstehen.
- Verwenden Sie die AWS Organizations `DisableAWSServiceAccess` API nicht, um den AWS Control Tower Tower-Servicezugriff auf die Organisation zu deaktivieren, in der Sie Ihre landing zone eingerichtet haben. Wenn Sie dies tun, funktionieren bestimmte Funktionen zur Erkennung von Drift in AWS Control Tower möglicherweise nicht richtig, wenn Sie keine Messaging-Unterstützung von erhalten AWS Organizations. Diese Funktionen zur Erkennung von Abweichungen tragen dazu bei, dass AWS Control Tower den Compliance-Status der Organisationseinheiten, Konten und Kontrollen in Ihrem Unternehmen genau melden kann. Weitere Informationen finden Sie API_DisableAWSServiceAccessin der AWS Organizations API-Referenz.
- Im Allgemeinen führt AWS Control Tower jeweils eine einzelne Aktion aus, die abgeschlossen sein muss, bevor eine weitere Aktion beginnen kann. Wenn Sie beispielsweise versuchen, ein Konto bereitzustellen, während der Prozess zur Aktivierung einer Steuerung bereits läuft, schlägt die Kontobereitstellung fehl.

  Ausnahme:

  - AWS Control Tower ermöglicht gleichzeitige Aktionen zur Bereitstellung optionaler Kontrollen. Weitere Informationen finden Sie unter Gleichzeitige Bereitstellung für optionale Kontrollen.
  - AWS Control Tower ermöglicht mit Account Factory bis zu zehn gleichzeitige Erstellungs-, Aktualisierungs- oder Registrierungsaktionen für Konten.

> **Note**
>
> Weitere Informationen zu den von AWS Control Tower erstellten Ressourcen finden Sie unterWas sind die gemeinsamen Konten?.

Tipps zu Konten und Organisationseinheiten

- Wir empfehlen, für jede registrierte Organisationseinheit maximal 1000 Konten zu verwenden, sodass Sie diese Konten mit der Re-register OU-Funktion aktualisieren können, wann immer

Kontoaktualisierungen erforderlich sind, z. B. wenn Sie neue Regionen für die Verwaltung konfigurieren.

- Um den Zeitaufwand für die Registrierung einer Organisationseinheit zu reduzieren, empfehlen wir, die Anzahl der Konten pro OU auf etwa 680 zu belassen, obwohl das Limit bei 1000 Konten pro OU liegt. In der Regel steigt der Zeitaufwand für die Registrierung einer Organisationseinheit mit der Anzahl der Regionen, in denen Ihre Organisationseinheit betrieben wird, multipliziert mit der Anzahl der Konten in der Organisationseinheit.
- Schätzungen zufolge kann eine Organisationseinheit mit 680 Konten bis zu 2 Stunden benötigen, um sich zu registrieren und die Kontrollen zu aktivieren, und bis zu 1 Stunde, um sich erneut zu registrieren. Außerdem dauert die Registrierung einer Organisationseinheit mit vielen Kontrollen länger als die Registrierung einer Organisationseinheit mit wenigen Kontrollen.
- Ein Problem bei der Festlegung eines längeren Zeitrahmens für die Registrierung einer Organisationseinheit besteht darin, dass dieser Prozess andere Aktionen blockiert. Einigen Kunden gefällt es, längere Zeiträume für die Registrierung oder erneute Registrierung einer Organisationseinheit einzuplanen, da sie es vorziehen, mehr Konten in jeder Organisationseinheit zuzulassen.

Wann sollten Sie sich als Root-Benutzer anmelden

Für bestimmte administrative Aufgaben müssen Sie sich als Stammbenutzer anmelden. Sie können sich als Root-Benutzer bei einem anmelden AWS-Konto , der von Account Factory in AWS Control Tower erstellt wurde.

Sie müssen sich als Stammbenutzer anmelden, um die folgenden Aktionen ausführen zu können:

- Ändern Sie bestimmte Kontoeinstellungen, einschließlich des Kontonamens, des Stammbenutzer-Passworts oder der E-Mail-Adresse. Weitere Informationen finden Sie unter Konten mit AWS Control Tower aktualisieren und verschieben.
- Um einen zu schließen AWS-Konto.
- Weitere Informationen zu Aktionen, für die Root-Benutzeranmeldedaten erforderlich sind, finden Sie im AWS -Kontenverwaltung Referenzhandbuch unter Aufgaben, für die Root-Benutzeranmeldedaten erforderlich sind.

> **Note**
>
> Um Ihren AWS Support-Plan zu ändern oder zu aktivieren, müssen Sie als Root-Benutzer angemeldet sein oder über die entsprechenden IAM-Berechtigungen verfügen. .

So melden Sie sich als Stammbenutzer an

1. Öffnen Sie die AWS Anmeldeseite.

   Wenn Sie nicht über die E-Mail-Adresse verfügen, auf die AWS-Konto Sie Zugriff benötigen, können Sie sie von AWS Control Tower abrufen. Öffnen Sie die Konsole für das Verwaltungskonto, wählen Sie Konten und suchen Sie nach der E-Mail-Adresse.
2. Geben Sie die E-Mail-Adresse des Benutzers ein, AWS-Konto auf das Sie Zugriff benötigen, und wählen Sie dann Weiter.
3. Wählen Sie Forgot password? (Passwort vergessen?), um zu veranlassen, dass Anweisungen zum Zurücksetzen des Passworts an die E-Mail-Adresse des Stammbenutzers gesendet werden.
4. Öffnen Sie die E-Mail-Nachricht zum Zurücksetzen des Passworts aus dem Stammbenutzerpostfach und folgen Sie dann den Anweisungen zum Zurücksetzen des Passworts.
5. Öffnen Sie die AWS Anmeldeseite und melden Sie sich mit Ihrem zurückgesetzten Passwort an.

Alternativ können Sie die AWS Root-Zugriffsverwaltungsfunktion verwenden, mit der Root-Aktionen an Mitgliedskonten ausgeführt werden können, ohne sich als Root anmelden zu müssen. Weitere Informationen finden Sie unter Zentrale Verwaltung des Root-Zugriffs für Kunden, die AWS Organizations

AWS Organizations Anleitungen

AWS Control Tower ist eng mit verbunden AWS Organizations. Im Folgenden finden Sie einige spezifische Hinweise dazu, wie sie am besten zusammenarbeiten, um Ihre AWS Umgebung zu schützen.

- In der AWS Organizations Dokumentation finden Sie Hinweise zu bewährten Methoden zum Schutz der Sicherheit Ihres AWS Control Tower Tower-Verwaltungskontos und Ihrer Mitgliedskonten.

  - Bewährte Methoden für das Verwaltungskonto
  - Bewährte Methoden für Mitgliedskonten
- Ändern oder trennen Sie nicht die Service Control Policies (SCPs), die AWS Control Tower für eine registrierte OU erstellt. Das Ändern oder Trennen dieser SCPs kann dazu führen, dass die Kontrollen in einen unbekannten Zustand übergehen. In diesem Fall müssen Sie Ihre landing zone zurücksetzen oder Ihre Organisationseinheit erneut in AWS Control Tower registrieren. Verwenden Sie stattdessen, AWS Organizations um neue SCPs zu erstellen und sie an die OU anzuhängen.
- Das Verschieben einzelner, bereits registrierter Konten von außerhalb einer registrierten Organisationseinheit in den AWS Control Tower führt zu Abweichungen, die behoben werden müssen. Siehe Arten von Abweichungen in der Unternehmensführung.
- Wenn Sie AWS Organizations Konten innerhalb einer Organisation erstellen, einladen oder verschieben, die bei AWS Control Tower registriert ist, werden diese Konten nicht von AWS Control Tower registriert und diese Änderungen werden nicht aufgezeichnet. Wenn Sie über SSO Zugriff auf diese Konten benötigen, finden Sie weitere Informationen unter Zugriff auf Mitgliedskonten.
- Wenn Sie AWS Organizations früher eine Organisationseinheit in eine von AWS Control Tower erstellte Organisation verschieben, wird die externe Organisationseinheit nicht von AWS Control Tower registriert.
- AWS Control Tower behandelt die Rechtefilterung anders als AWS Organizations bisher. Wenn Ihre Konten mit AWS Control Tower Account Factory bereitgestellt werden, können Endbenutzer die Namen und übergeordneten Einheiten aller Organisationseinheiten in der AWS Control Tower Tower-Konsole sehen, auch wenn sie nicht berechtigt sind, diese Namen und Eltern direkt abzurufen. AWS Organizations
- AWS Control Tower unterstützt keine gemischten Berechtigungen für Organisationen, wie z. B. die Erlaubnis, die übergeordnete Organisationseinheit einer Organisationseinheit anzuzeigen, aber nicht die Namen von Organisationseinheiten einzusehen. Aus diesem Grund wird von AWS Control Tower Tower-Administratoren erwartet, dass sie über volle Berechtigungen verfügen.
- Das AWS Organizations `FullAWSAccess` SCP muss angewendet werden und sollte nicht mit anderen SCPs zusammengeführt werden. Änderungen an diesem SCP werden nicht als Abweichung gemeldet. Einige Änderungen können jedoch die Funktionalität von AWS Control Tower auf unvorhersehbare Weise beeinträchtigen, wenn der Zugriff auf bestimmte Ressourcen verweigert wird. Wenn der SCP beispielsweise getrennt oder geändert wird, kann ein Konto den Zugriff auf einen AWS Config Rekorder verlieren oder eine Lücke in CloudTrail der Protokollierung entstehen.

- Verwenden Sie die AWS Organizations `DisableAWSServiceAccess` API nicht, um den AWS Control Tower Tower-Servicezugriff auf die Organisation zu deaktivieren, in der Sie Ihre landing zone eingerichtet haben. Wenn Sie dies tun, funktionieren bestimmte Funktionen zur Erkennung von Drift in AWS Control Tower möglicherweise nicht richtig, wenn Sie keine Messaging-Unterstützung von erhalten AWS Organizations. Diese Funktionen zur Erkennung von Abweichungen tragen dazu bei, dass AWS Control Tower den Compliance-Status der Organisationseinheiten, Konten und Kontrollen in Ihrem Unternehmen genau melden kann. Weitere Informationen finden Sie API_DisableAWSServiceAccessin der AWS Organizations API-Referenz.

Anleitung zum IAM Identity Center

AWS Control Tower empfiehlt, dass Sie AWS Identity and Access Management (IAM) verwenden, um den Zugriff auf Ihre AWS-Konten zu regulieren. Sie haben jedoch die Möglichkeit zu wählen, ob AWS Control Tower das IAM Identity Center für Sie einrichtet, ob Sie IAM Identity Center für sich selbst einrichten, und zwar so, dass es Ihren Geschäftsanforderungen am effektivsten entspricht, oder ob Sie eine andere Methode für den Kontozugriff wählen möchten.

> **Note**
>
> SSO ist eine Abkürzung, die in der Technologiebranche für Single Sign-On verwendet wird. Im Allgemeinen ist SSO ein Dienst zur Sitzungs- und Benutzerauthentifizierung. Es ermöglicht jemandem, einen Satz von Anmeldeinformationen für den Zugriff auf viele Anwendungen zu verwenden. Wenn wir uns auf die Single-Sign-On-Funktion in beziehen AWS, beziehen wir uns auf den AWS Dienst, der als IAM oder IAM Identity AWS Identity and Access ManagementCenter bezeichnet wird und als IAM Identity Center abgekürzt wird.

Standardmäßig richtet AWS Control Tower das AWS IAM Identity Center für Ihre landing zone ein. Dies entspricht den Best-Practices-Richtlinien, die unter Organisieren Ihrer AWS Umgebung mithilfe mehrerer Konten definiert sind. Die meisten Kunden wählen die Standardeinstellung. Manchmal sind alternative Zugriffsmethoden erforderlich, um die Einhaltung gesetzlicher Vorschriften in bestimmten Branchen oder Ländern zu gewährleisten oder AWS-Regionen wenn AWS IAM Identity Center nicht verfügbar ist.

Eine Option wählen

Von der Konsole aus können Sie wählen, ob Sie das IAM Identity Center während der Einrichtung der landing zone selbst verwalten möchten, anstatt es AWS Control Tower zu überlassen, es für

Sie einzurichten. Sie können diese Auswahl jederzeit später ändern, indem Sie die Landingzone-Einstellungen ändern und Ihre Landingzone auf der Seite Landingzone-Einstellungen aktualisieren.

Um abzubrechen AWS IAM Identity Center in AWS Control Tower oder um mit der Nutzung zu beginnen AWS IAM Identity Center

1. Navigiere zur Seite mit den Einstellungen für die landing zone
2. Wählen Sie die Registerkarte Konfigurationen
3. Wählen Sie dann das entsprechende Optionsfeld, um Ihre Auswahl für AWS IAM Identity Center zu ändern.

Nachdem Sie sich dafür entschieden haben, AWS IAM Identity Center als Ihren IdP selbst zu verwalten, erstellt AWS Control Tower nur die Rollen und Richtlinien, die für die Verwaltung von AWS Control Tower erforderlich sind, z. B. und. `AWSControlTowerAdmin` `AWSControlTowerAdminPolicy` Für Landing Zones, die sich selbst verwalten, erstellt AWS Control Tower keine IAM-Rollen und -Gruppierungen mehr für kundenspezifische Zwecke — weder bei der Einrichtung der landing zone noch bei der Kontobereitstellung mit Account Factory.

> **Note**
>
> Wenn Sie AWS IAM Identity Center aus Ihrer AWS Control Tower-Landing landing zone entfernen, werden die von AWS Control Tower erstellten Benutzer, Gruppen und Berechtigungssätze nicht entfernt. Wir empfehlen Ihnen, diese Ressourcen zu entfernen.

Account Factory Factory-Kunden mit alternativen Identitätsanbietern (IdPs) wie Azure AD, Ping oder Okta können dem AWS IAM Identity Center-Prozess folgen, um eine Verbindung zu einem externen Identitätsanbieter herzustellen und ihren IdP zu integrieren. Sie können jederzeit wieder dazu zurückkehren, dass AWS Control Tower Ihre Gruppierungen und Rollen generiert, indem Sie die Landingzone-Einstellungen ändern.

- Spezifische Informationen darüber, wie AWS Control Tower mit IAM Identity Center auf der Grundlage Ihrer Identitätsquelle zusammenarbeitet, finden Sie unter Überlegungen für AWS IAM Identity Center Kunden im Abschnitt Pre-launch Prüfungen auf der Seite Erste Schritte in diesem Benutzerhandbuch.

- Weitere Informationen darüber, wie das Verhalten von AWS Control Tower mit IAM Identity Center und verschiedenen Identitätsquellen interagiert, finden Sie unter Überlegungen zur Änderung Ihrer Identitätsquelle im IAM Identity Center-Benutzerhandbuch.
- Weitere Informationen Arbeiten mit AWS IAM Identity Center und AWS Control Tower zur Zusammenarbeit mit AWS Control Tower und IAM Identity Center finden Sie unter.

Anleitung von Account Factory

> **Note**
>
> Die Bereitstellung, Aktualisierung und Anpassung eines einzelnen Kontos muss auf eine Organisationseinheit (OU) abzielen, für die AWSControlTowerBaseline diese Option aktiviert ist. Wenn in einer Organisationseinheit das nicht AWSControlTowerBaseline aktiviert ist, können Sie die automatische Kontoregistrierung aktivieren oder ResetEnabledControl APIs auf ResetEnabledBaseline EnabledBaselines und EnabledControls auf dieser Organisationseinheit verwenden, um Konten zu registrieren. Einzelheiten zu finden Sie unter:. AWSControlTowerBaseline Basistypen, die auf OU-Ebene gelten

Bei der Verwendung von Account Factory zur Bereitstellung eines neuen Kontos in AWS Control Tower können Probleme auftreten. Informationen zur Behebung dieser Probleme finden Sie New Account Provisioning Failed (Bereitstellung eines neuen Kontos fehlgeschlagen) im Abschnitt zur Fehlerbehebung im AWS Control Tower Tower-Benutzerhandbuch.

Wir empfehlen, Verbundbenutzer oder IAM-Rollen anstelle von IAM-Benutzern zu erstellen. Verbundbenutzer und IAM-Rollen stellen Ihnen temporäre Anmeldeinformationen zur Verfügung. IAM-Benutzer verfügen über langfristige Anmeldeinformationen, deren Verwaltung sich als schwierig erweisen kann. Weitere Informationen finden Sie unter IAM-Identitäten (Benutzer, Benutzergruppen und Rollen) im IAM-Benutzerhandbuch.

Wenn Sie bei der Bereitstellung eines neuen Kontos in Account Factory oder bei der Verwendung der Kontoregistrierungsfunktion AWS Control Tower als IAM-Benutzer oder IAM Identity Center-Benutzer authentifiziert sind, stellen Sie sicher, dass Ihr Benutzer Zugriff auf Ihr Portfolio hat. AWS Service Catalog Andernfalls erhalten Sie möglicherweise eine Fehlermeldung von Service Catalog. Weitere Informationen finden Sie Portfoliofehler bei AWS Control Tower Account Factory im Abschnitt zur Fehlerbehebung im AWS Control Tower Tower-Benutzerhandbuch.

> **Note**
>
> Bei deaktivierter automatischer Registrierung: Bis zu fünf Konten können gleichzeitig bereitgestellt werden.
> Bei aktivierter automatischer Registrierung: Bis zu 5 Konten können gleichzeitig bereitgestellt werden, aber jeder aktive Kontoverschiebungsvorgang für die Ziel-OU blockiert die gesamte Bereitstellung auf derselben Organisationseinheit, bis sie abgeschlossen ist.

Hinweise zum Abonnieren von SNS-Themen

Abonnieren Sie SNS-Themen, um Informationen über Ihre AWS Control Tower Tower-Umgebung zu erhalten.

> **Note**
>
> AWS Control Tower wird das Senden von Drift-Benachrichtigungen an das SNS-Thema für alle Kunden auf LZ4.0 + einstellen.

- Das `aws-controltower-AllConfigNotifications` SNS-Thema empfängt alle Ereignisse, die von veröffentlicht wurden AWS Config, einschließlich Compliance-Benachrichtigungen und CloudWatch Amazon-Ereignisbenachrichtigungen. In diesem Thema werden Sie beispielsweise darüber informiert, ob ein Kontrollverstoß aufgetreten ist. Es enthält auch Informationen über andere Arten von Ereignissen. (Erfahren Sie mehr AWS Configdarüber, was sie veröffentlichen, wenn dieses Thema konfiguriert ist.)
- Datenereignisse aus dem `aws-controltower-BaselineCloudTrail` Trail sind so eingestellt, dass sie auch im `aws-controltower-AllConfigNotifications` SNS-Thema veröffentlicht werden.
- Um detaillierte Compliance-Benachrichtigungen zu erhalten, empfehlen wir Ihnen, das `aws-controltower-AllConfigNotifications` SNS-Thema zu abonnieren. In diesem Thema werden Compliance-Benachrichtigungen von allen Kinderkonten zusammengefasst.
- Um Drift-Benachrichtigungen und andere Benachrichtigungen sowie Compliance-Benachrichtigungen zu erhalten, aber insgesamt weniger Benachrichtigungen, empfehlen wir Ihnen, das `aws-controltower-AggregateSecurityNotifications` SNS-Thema zu abonnieren.

- Um Benachrichtigungen über Fehler in AWS Control Tower Account Factory for Terraform (AFT) zu erhalten, können Sie ein SNS-Thema mit dem Titel aft_failure_notifications, angezeigt im AFT-Repository abonnieren. Beispiel:

```
resource "aws_sns_topic" "aft_failure_notifications" {
    name = "aft-failure-notifications"
    kms_master_key_id = "alias/aws/sns"
}
```

- Alle SNS-Themen werden im Ruhezustand mit Festplattenverschlüsselung verschlüsselt. Weitere Informationen finden Sie unter Datenverschlüsselung.

Weitere Informationen zu SNS-Themen und Compliance finden Sie unter Prävention und Benachrichtigung.

Anleitung für KMS-Schlüssel

AWS Control Tower arbeitet mit AWS Key Management Service (AWS KMS). Wenn Sie Ihre AWS Control Tower Tower-Ressourcen mit einem von Ihnen verwalteten Verschlüsselungsschlüssel ver- und entschlüsseln möchten, können Sie ihn optional generieren und konfigurieren. AWS KMS keys Sie können jederzeit einen KMS-Schlüssel hinzufügen oder ändern, wenn Sie Ihre landing zone aktualisieren. Als bewährte Methode empfehlen wir, Ihre eigenen KMS-Schlüssel zu verwenden und diese von Zeit zu Zeit zu ändern.

AWS KMS ermöglicht es Ihnen, KMS-Schlüssel und asymmetrische Schlüssel für mehrere Regionen zu erstellen. AWS Control Tower unterstützt jedoch keine Schlüssel für mehrere Regionen oder asymmetrische Schlüssel. AWS Control Tower führt eine Vorabprüfung Ihrer vorhandenen Schlüssel durch. Möglicherweise wird eine Fehlermeldung angezeigt, wenn Sie einen Schlüssel für mehrere Regionen oder einen asymmetrischen Schlüssel auswählen. Generieren Sie in diesem Fall einen weiteren Schlüssel zur Verwendung mit AWS Control Tower Tower-Ressourcen.

Für Kunden, die einen AWS CloudHSM-Cluster betreiben: Erstellen Sie einen benutzerdefinierten Schlüsselspeicher, der Ihrem CloudHSM-Cluster zugeordnet ist. Anschließend können Sie einen KMS-Schlüssel erstellen, der sich in dem von Ihnen erstellten benutzerdefinierten CloudHSM-Schlüsselspeicher befindet. Sie können diesen KMS-Schlüssel zu AWS Control Tower hinzufügen.

Sie müssen die Berechtigungsrichtlinie eines KMS-Schlüssels speziell aktualisieren, damit er mit AWS Control Tower funktioniert. Einzelheiten finden Sie im Abschnitt mit dem TitelAktualisieren Sie die KMS-Schlüsselrichtlinie.

Bewährte Methoden für Landezonenupdates

In diesem Abschnitt finden Sie einige Überlegungen und bewährte Methoden, die Sie berücksichtigen sollten, wenn Sie ein Upgrade Ihrer landing zone Zone-Version in AWS Control Tower in Betracht ziehen. Der Wechsel von der Landezone-Versionsserie 2.0 zur Landezone-Versionsserie 3.0 ist besonders wichtig. Wenn Sie Ihre landing zone aktualisieren, werden Sie von AWS Control Tower automatisch auf die neueste verfügbare Version umgestellt.

> **Note**
>
> Es hat sich bewährt, auf die neueste Version der landing zone zu aktualisieren.

Zusammenfassung der in diesem Abschnitt erläuterten bewährten Verfahren

- Bewährtes Verfahren: Aus Sicherheits- und Auditgründen empfehlen wir dringend, die Protokollierung generell für alle Konten zu aktivieren und die Protokollierungsinformationen an einen zentralen Ort zu senden. In AWS Control Tower ist dieser zentrale Ort das Log-Archive-Konto, das einen Amazon S3 S3-Logging-Bucket bereitstellt.
- Bewährtes Verfahren: Wenn Sie den CloudTrail Trail auf Organisationsebene in AWS Control Tower deaktivieren, richten Sie Ihre eigenen Trails ein und verwalten Sie sie.
- Bewährtes Verfahren: Richten Sie beim Betrieb Ihrer AWS Control Tower Tower-Umgebung eine Testumgebung ein.

Vorteile der Umstellung von 2.x-Landingzone-Versionen auf 3.x-Landezone-Versionen

- Erfassen Sie AWS Config Ressourcen nur in der Heimatregion, was zu Kosteneinsparungen führt, wenn Sie globale Ressourcen verwalten
- Verschlüsseln Sie Ihren AWS CloudTrail Trail mit Ihrem eigenen KMS-Schlüssel
- Passen Sie Ihren Zeitrahmen für die Aufbewahrung von Protokollen an
- Verbesserte obligatorische Kontrollen
- Höhere Anzahl verfügbarer Kontrollen
- Integriert mit AWS Security Hub CSPM
- Python-Laufzeitaktualisierungen

Vorbehalte beim Wechsel von 2.x-Landingzone-Versionen zu 3.x-Landingzone-Versionen

- Mit landing zone 3.0 und höher unterstützt AWS Control Tower keine verwalteten AWS CloudTrail Trails auf Kontoebene mehr. AWS
- Sie haben die Möglichkeit, einen von AWS Control Tower verwalteten Trail auf Organisationsebene zu wählen oder ihn zu deaktivieren und Ihre eigenen CloudTrail Trails zu verwalten.
- Es besteht ein gewisses Potenzial für doppelte Kosten, insbesondere wenn einige Konten innerhalb einer Organisationseinheit nicht bei AWS Control Tower registriert sind und eigene Trails auf Kontoebene haben, die Sie behalten möchten.

Überlegungen zur Auswahl von Trails auf Organisationsebene CloudTrail

- Wenn Sie ein Upgrade auf 3.0 oder höher durchführen, löscht AWS Control Tower die ursprünglich erstellten Trails auf Kontoebene nach 24 Stunden. [Ausnahme]
- Es gehen keine Daten von diesen Spuren verloren. Ihre vorhandenen Protokolle bleiben erhalten, auch wenn die Spuren entfernt werden.
- AWS Control Tower erstellt in demselben Amazon S3 S3-Bucket einen neuen Pfad für die Trails, um Trails auf Kontoebene von Trails auf Organisationsebene zu unterscheiden.
  - Ein Protokollpfad für Konto-Trails hat die folgende Form: `/orgId/AWSLogs/...`
  - Ein Protokollpfad für ein Unternehmen hat die folgende Form: `/orgId/AWSLogs/orgId/...`
- Zusätzliche CloudTrail Trails, die Sie bereitgestellt haben, Trails, die nicht von AWS Control Tower bereitgestellt wurden, werden nicht berührt.
- Alle Konten sind im Trail auf Organisationsebene enthalten — auch Konten, die nicht im AWS Control Tower registriert sind —, wenn die nicht registrierten Konten Teil einer registrierten Organisationseinheit sind.
- CloudWatch Amazon-Alarme in verknüpften Konten werden nicht ausgelöst.
- Wenn Sie sich von einem Trail auf Organisationsebene abmelden, erstellt AWS Control Tower den Trail trotzdem, setzt seinen Status jedoch auf Aus.
- Als bewährte Methode sollten Sie, wenn Sie den Trail auf Organisationsebene in AWS Control Tower deaktivieren, Ihre eigenen CloudTrail Trails einrichten und verwalten.

Vorteile von Trails auf Organisationsebene

- Der Organisationspfad funktioniert für alle Konten in der Organisationseinheit.

- Die protokollierten Elemente sind standardisiert und können von Kontobenutzern nicht geändert werden.

Stellen Sie sich eine Testumgebung vor

Wenn Sie Ihre landing zone aktualisieren, nimmt AWS Control Tower nur Änderungen an den gemeinsamen Konten und der Foundational OU vor. Es werden keine Änderungen an Ihren Workload-Konten oder Organisationseinheiten vorgenommen. Als bewährte Methode empfehlen wir Ihnen jedoch, beim Betrieb Ihrer AWS Control Tower Tower-Umgebung eine Testumgebung einzurichten. In der isolierten Testumgebung können Sie die landing zone Zone-Upgrades von AWS Control Tower sowie alle Änderungen testen, die Sie an den Service Control Policies (SCPs) vornehmen, und Sie können die Kontrollen testen, die Sie auf die Umgebung anwenden möchten. Diese Empfehlung ist besonders hilfreich, wenn Sie in einer regulierten Branche tätig sind.

Checkliste für häufig auftretende Fehler bei der Aktualisierung

Im Folgenden finden Sie eine kurze Liste von Aufgaben, die Sie ausführen können, um häufige Fehler bei der Aktualisierung Ihrer AWS Control Tower Tower-Landing landing zone von 2.x-Versionen auf 3.x-Versionen zu vermeiden.

Grundlegende Checkliste für Updates

- Überprüfe deine landing zone:

  — Rufen Sie den AWS Control Tower Tower-Service auf, überprüfen Sie die Seiten Organisationseinheiten und Konten und vergewissern Sie sich, dass Ihr Kontostatus auf Registriert und registriert gesetzt ist.

  — Falls zutreffend, überprüfen und bestätigen Sie, dass der letzte Durchlauf Ihrer Anpassungspipeline erfolgreich war.

  — Überprüfen Sie den zentralen Amazon S3 S3-Logging-Bucket im Audit-Konto, da alle zuvor an der Bucket-Richtlinie vorgenommenen Änderungen überschrieben werden.
- Stellen Sie sicher, dass SCPs, die nicht im Besitz von AWS Control Tower sind, die `AWSControlTowerExecution` Rolle nicht daran hindern, Aktionen in Mitgliedskonten oder Aktionen im Verwaltungskonto für die Administratorrolle auszuführen, die das Update durchführt.

AI-based Services und AWS Control Tower

Sie können Richtlinien zur Servicesteuerung (Service Control Policies, SCPs) erstellen, mit denen Sie die Speicherung Ihrer Daten durch AI-based Dienste auf AWS deaktivieren können. Diese SCP-Richtlinien legen fest, dass AI-based Dienste wie Amazon Rekognition oder Amazon Ihre Daten nicht speichern und verwenden können CodeWhisperer, um andere Dienste zu verbessern. AI-based AWS

Diese AI-Opt-Out-SCP-Richtlinien können für Ihr gesamtes Unternehmen, für eine Organisationseinheit oder für ein bestimmtes Konto gelten. Die Richtlinien sind global gültig. Weitere Informationen zu diesen Richtlinien finden Sie in der AWS Organizations Dokumentation unter Richtlinien zur Deaktivierung von KI-Diensten.

Eine Liste der AWS Dienste, die KI verwenden, sowie Beispiele für Richtlinien finden Sie im AWS Organizations Benutzerhandbuch unter Syntax und Beispiele für Opt-Out-Richtlinien für KI-Dienste.

Verwaltung von Konfigurationsupdates in AWS Control Tower

Es liegt in der Verantwortung der Mitglieder Ihres zentralen Cloud-Administratorteams, Ihre landing zone auf dem neuesten Stand zu halten. Durch die Aktualisierung Ihrer landing zone wird sichergestellt, dass AWS Control Tower gepatcht und aktualisiert ist. Um Ihre landing zone vor potenziellen Compliance-Problemen zu schützen, sollten die Mitglieder des zentralen Cloud-Administratorteams außerdem Drift-Probleme lösen, sobald sie erkannt und gemeldet werden.

> **Note**
>
> Die AWS Control Tower Tower-Konsole zeigt an, wann Ihre landing zone aktualisiert werden muss. Wenn du keine Option zum Aktualisieren siehst, ist deine landing zone bereits auf dem neuesten Stand.

Die folgende Tabelle enthält eine Liste der Aktualisierungsversionen für die AWS Control Tower landing zone mit Links zu Beschreibungen der einzelnen Versionen.

Version	Datum der Veröffentlichung	Description
4,0	17.11.2025	Landezone Version 4.0
3.3	12.12.2023	Landezone Version 3.3
3.2	6-09-2023	Landezone Version 3.2
3.1	2-09-2023	Landezone Version 3.1
3.0	26.7.2022	Landezone Version 3.0
2.9	22.4.2022	Landezone Version 2.9
2.8	2-10-2022	Landezone Version 2.8
2.7	4-8-2021	Landezone Version 2.7
2.6	29.12.2020	Landezone Version 2.6

Version	Datum der Veröffentlichung	Description
2.5	18.11.2020	Landezone Version 2.5
2.4	Keine	Keine
2.3	3-5-2020	Landezone Version 2.3
2.2	11-13-19	Landezone Version 2.2
2.1	6-24-19	Landezone Version 2.1

Jedes Mal, wenn Sie Ihre landing zone aktualisieren, haben Sie die Möglichkeit, Ihre Landezoneneinstellungen zu ändern.

Vorteile der Aktualisierung

- Sie können Ihre verwalteten Regionen ändern
- Sie können Ihre Richtlinien zur Aufbewahrung von Protokollen ändern
- Sie können die Option Region Deny Control hinzufügen oder entfernen
- Sie können AWS KMS-Verschlüsselungsschlüssel anwenden
- Sie können Ihren Trail auf Organisationsebene CloudTrail aktivieren oder deaktivieren.
- Sie können die Landezonendrift beheben

Wenn Sie Ihre landing zone aktualisieren, erhalten Sie automatisch die neuesten Funktionen für AWS Control Tower. Sehen Sie sich Ihre aktuelle Landingzone-Version auf der Seite mit den Landingzone-Einstellungen an.

Wenn ein Update fehlschlägt, führt AWS Control Tower kein Rollback zu einer früheren landing zone Zone-Version durch. Möglicherweise befindet sich Ihre landing zone in einem unbestimmten Zustand. Wenn ja, wenden Sie sich an den Support AWS . Weitere Informationen zur Behebung eines Fehlers bei der Aktualisierung finden Sie unterDie Landing Zone konnte nicht aktualisiert werden.

Sie haben die Möglichkeit, ungenutzte AWS Identity Center-Zuordnungen (früher AWS SSO genannt) zu löschen, wenn Sie Ihre landing zone aktualisieren. Weitere Informationen finden Sie unter Feldnotizen: Automatisches Löschen ungenutzter IAM Identity Center-Zuordnungen während AWS Control Tower Tower-Upgrades.

Voraussetzung für Update und Reset — deaktivieren Sie Requester Pays

Bevor Sie Ihre landing zone aktualisieren oder zurücksetzen, stellen Sie sicher, dass im Amazon S3 S3-Logging-Bucket für das Log Archive-Konto die Funktion Requester Pays nicht aktiviert ist. Sie müssen diese Funktion ausschalten, bevor Sie mit dem Aktualisierungs - oder Reset-Vorgang beginnen. Wenn AWS Control Tower Ihren Logging-Bucket einrichtet, ist diese Funktion nicht aktiviert. Daher müssen nur die Kunden, die die Funktion „Requester Pays“ anschließend aktiviert haben, sie deaktivieren. Weitere Informationen finden Sie in den Amazon S3 S3-Bucket-Richtlinien für CloudTrail und unter Using Requester Pays Buckets.

Über Landezone-Updates

Updates sind erforderlich, um Abweichungen in der Unternehmensführung zu korrigieren oder um auf eine neue Version von AWS Control Tower umzusteigen. Um ein vollständiges Update von AWS Control Tower durchzuführen, müssen Sie zuerst Ihre landing zone und dann die registrierten Konten einzeln aktualisieren. Möglicherweise müssen Sie drei Arten von Aktualisierungen zu verschiedenen Zeiten durchführen.

- Ein Landingzone-Update: In den meisten Fällen wird diese Art von Update durchgeführt, indem Sie auf der Seite mit den Landingzone-Einstellungen die Option Update auswählen. Möglicherweise müssen Sie eine Aktualisierung der landing zone durchführen, um bestimmte Drifttypen zu beheben, und Sie können bei Bedarf „Zurücksetzen“ wählen.
- Aktualisierung eines oder mehrerer einzelner Konten: Sie müssen Konten aktualisieren, wenn sich die zugehörigen Informationen ändern oder bestimmte Arten von Abweichungen aufgetreten sind. Wenn ein Konto aktualisiert werden muss, zeigt der Status des Kontos auf der Seite Konten die Meldung Update verfügbar an.

  Um ein einzelnes Konto zu aktualisieren, navigieren Sie zur Kontodetailseite und wählen Sie Konto aktualisieren aus. Konten können auch manuell, durch Auswahl der Re-register Organisationseinheit oder mithilfe eines automatisierten Skripting-Ansatzes aktualisiert werden, der in einem späteren Abschnitt dieser Seite beschrieben wird.
- Ein vollständiges Update: Ein vollständiges Update beinhaltet eine Aktualisierung Ihrer landing zone, gefolgt von einer Aktualisierung aller registrierten Konten in Ihren registrierten Organisationseinheiten. Bei einer neuen Version von AWS Control Tower wie 3.0, 3.2 usw. sind vollständige Updates erforderlich. Um den vollständigen Aktualisierungsprozess zu vereinfachen, können Sie für Organisationseinheiten mit 1000 oder weniger Konten Re-register OU auswählen,

um alle Konten innerhalb dieser Organisationseinheit zu aktualisieren, und den Re-registerOU-Befehl für jede OU wiederholen.

Weitere Informationen zu Landezonenaktualisierungen finden Sie unter Bewährte Methoden für Landezonenaktualisierungen.

> **Note**
>
> Nach Abschluss eines landing zone Zone-Updates können Sie das Update oder das Downgrade auf eine frühere Version nicht rückgängig machen.

Aktualisiere deine landing zone

Am einfachsten können Sie Ihre AWS Control Tower Tower-Landingzone über die Seite mit den Landingzone-Einstellungen aktualisieren, die Sie erreichen können, indem Sie im linken Navigationsbereich des AWS Control Tower Tower-Dashboards Landingzone-Einstellungen wählen.

Die Seite mit den Landingzone-Einstellungen zeigt Ihnen die aktuelle Version Ihrer Landing Zone und listet alle aktualisierten Versionen auf, die möglicherweise verfügbar sind. Sie können die Schaltfläche Update (Aktualisieren) auswählen, wenn Sie Ihre Version aktualisieren müssen.

> **Note**
>
> Alternativ können Sie Ihre Landing Zone manuell aktualisieren. Das Update dauert ungefähr gleich lang, unabhängig davon, ob Sie die Schaltfläche Update (Aktualisieren) oder den manuellen Vorgang verwenden. Informationen zur manuellen Aktualisierung Ihrer Landing Zone finden Sie in den folgenden Schritten 1 und 2.

Standardverfahren für Updates

Das folgende Verfahren führt Sie durch die Schritte eines vollständigen Updates für AWS Control Tower von der Konsole aus. Informationen zum Aktualisieren eines einzelnen Kontos finden Sie unterAktualisiere das Konto in der Konsole.

Um deine landing zone mit einer beliebigen Anzahl von Konten pro OU zu aktualisieren

1. Öffnen Sie einen Webbrowser und navigieren Sie zur AWS Control Tower Tower-Konsole unter https://console.aws.amazon.com/controltower/home/update.
2. Überprüfen Sie die Informationen im Assistenten und wählen Sie Update aus. Dadurch werden das Backend der landing zone sowie Ihre gemeinsamen Konten aktualisiert. Dieser Vorgang kann etwas mehr als eine halbe Stunde dauern.
3. Aktualisieren Sie Ihre Mitgliedskonten (dieses Verfahren muss für eine Organisationseinheit mit mehr als 1000 Konten befolgt werden).
4. Wählen Sie im linken Navigationsbereich Organisation aus.
5. Gehen Sie wie unter beschrieben vor, um jedes Konto zu aktualisierenAktualisiere das Konto in der Konsole.

> **Optional Re-register OU zum Aktualisieren von Konten**
>
> Für registrierte AWS Control Tower Tower-Organisationseinheiten mit weniger als 1000 Konten können Sie die OU-Seite im Dashboard aufrufen und Re-registerOU auswählen, um die Konten in dieser OU zu aktualisieren.

Wählen Sie eine Landezonenversion

Wenn Sie die AWS Control Tower landing zone Version 3.1 und höher verwenden, können Sie wählen, ob Sie bei der aktuellen Version bleiben oder ein Upgrade auf eine neuere Version durchführen möchten, wenn Sie einen Update - oder Reset-Vorgang für Ihre landing zone Zone-Konfigurationen durchführen. Der Reset-Vorgang ist in den meisten Situationen der beste Weg, um Drift zu reparieren.

Sie können eine Landingzone-Version in der AWS Control Tower Tower-Konsole oder mithilfe der AWS Control Tower Tower-APIs auswählen.

> **Note**
>
> Wenn Sie sich für die Bereitstellung einer landing zone Zone-Version entscheiden, die eine Zwischenversion überspringt, z. B. wenn Sie von 3.1 auf 3.3 wechseln, stellt AWS Control Tower die Zwischenversion automatisch als Teil des Aktualisierungsvorgangs bereit.

In der Konversation wird die Umstellung auf eine neuere Version oft als Upgrade und nicht nur als Update bezeichnet. Diese beiden Konzepte unterscheiden sich, da Sie Ihre Landingzone-Einstellungen aktualisieren können, ohne auf eine neue Version zu aktualisieren, indem Sie beispielsweise die Regionen ändern, für die Sie zuständig sind. In der Konsole führt die Schaltfläche Update ein direktes Update oder einen Upgrade-Vorgang aus, der auf Ihrer aktuellen Landingzone-Version und der Version, die Sie bereitstellen möchten, basiert.

Wählen Sie Ihre Landezone-Version — Konsolenprozedur

1. Navigieren Sie von der AWS Control Tower Tower-Konsole aus zur Seite mit den Einstellungen für die Landing Zone. Wählen Sie in der Tabelle der verfügbaren Landing Zones die neue Version aus. Denken Sie daran, dass Sie Versionen 3.1 oder höher auswählen können. Versionen vor 3.1 sind mit dieser Funktion nicht kompatibel.
2. Wenn Sie eine Version aus der Tabelle auswählen, können Sie die verfügbaren Aktionen sehen. Das Update ist verfügbar, wenn Ihre aktuelle Version älter als die ausgewählte Version ist. Reset ist verfügbar, wenn Ihre aktuelle Version 3.1 oder neuer ist.
3. Nachdem Sie die Version ausgewählt haben, klicken Sie oben rechts auf dem Bildschirm auf die Schaltfläche Aktualisieren oder Zurücksetzen.
4. Sie sehen eine Bestätigungsanzeige mit der landing zone Zone-Version, die Sie für den Einsatz ausgewählt haben. Um fortzufahren, wählen Sie unten rechts Weiter aus. Ihr Aktualisierungsvorgang kann einige Minuten oder länger dauern.
5. Nachdem die landing zone aktualisiert wurde, müssen Sie möglicherweise Ihre registrierten Organisationseinheiten aktualisieren. Um eine Organisationseinheit zu aktualisieren, müssen Sie sie mithilfe des Re-register OU-Prozesses erneut registrieren. Re-registering Eine Organisationseinheit wendet die aktualisierte Baseline auf alle Konten in dieser Organisationseinheit an.

Kontoaktualisierungen, Landingzone-Versionen und Baselines

AWS Control Tower Tower-Landezonen sind AWS Ressourcen, die einer Reihe von Basiskonfigurationen entsprechen. Es gibt keine Eins-zu-Eins-Zuordnung von Baselines und landing zone Zone-Versionen. Sie können sich eine Tabelle ansehen, die Folgendes zeigt. Kompatibilität von OU-Baselines und landing zone Zone-Versionen

Wenn Sie zu einer Basisversion wechseln, müssen Sie Ihre Konten nach dem landing zone Zone-Update aktualisieren. Wenn Sie beispielsweise von 3.1 auf 3.2 aktualisieren, müssten Sie Ihre Konten nicht aktualisieren, da diese landing zone Zone-Versionen dieselbe Baseline verwenden.

Im Gegensatz dazu müssten Sie bei einem Upgrade von 3.1 auf 3.3 Konten aktualisieren, da die Basisversion 4.0 ist, die 3.2 auf 3.3 umfasst.

Weitere Informationen zur Beziehung zwischen landing zone Zone-Versionen und Baselines finden Sie unter. Kompatibilität von OU-Baselines und landing zone Zone-Versionen

AWS CloudTrail Spuren während der Landezonenaktualisierung beibehalten

Sie können sich dafür entscheiden, Ihre AWS CloudTrail Trails auf Kontoebene beizubehalten, wenn Sie Ihre AWS Control Tower Tower-Landing Zone-Version aktualisieren.

Voraussetzungen

- Ihre landing zone Zone-Version ist kleiner als 3.0.
- Ihr letzter Erstellungs - oder Aktualisierungsvorgang war erfolgreich.

Um den Trail auf Kontoebene beizubehalten und sich für Trails auf Organisationsebene anzumelden CloudTrail

1. Wenden Sie sich mit der Bitte, Ihr Konto auf die Zulassungsliste zu setzen, an den AWS Support.
2. Das Support-Team bestätigt, wann das Zielkonto auf der Zulassungsliste steht.
3. Aktualisieren Sie nach der Bestätigung Ihre landing zone auf Version 3.1 oder höher und wählen Sie AWS CloudTrail Konfiguration — Aktiviert.

Um den Trail auf Kontoebene beizubehalten und sich von den von AWS Control Tower verwalteten CloudTrail Trails abzumelden

1. Wenden Sie sich mit der Bitte, Ihr Konto auf die Zulassungsliste zu setzen, an den AWS Support.
2. Das Support-Team bestätigt, wann das Zielkonto auf der Zulassungsliste steht.
3. Aktualisieren Sie nach der Bestätigung Ihre landing zone auf Version 3.1 oder höher und wählen Sie AWS CloudTrail Konfiguration — Nicht aktiviert.

> **Important**
>
> Nachdem die CloudTrail Trails auf Kontoebene beibehalten wurden, können wir keine Trails mehr entfernen oder deine Accounts von der Zulassungsliste entfernen.

Wie stellst du eine Support-Anfrage, um deine Trails auf Kontoebene beizubehalten

Wenn Sie während eines Landing Zone-Updates Trails auf Kontoebene behalten müssen, müssen Sie sich an den AWS Support wenden, um Ihr Konto zur AWS Control Tower Tower-Zulassungsliste hinzuzufügen. Gehen Sie wie folgt vor, um ein Support-Ticket einzureichen:

1. Melden Sie sich bei der AWS Management Console an.
2. Navigieren Sie zum AWS Support Center.
3. Wählen Sie Create case (Fall erstellen) aus.
4. Wählen Sie als Falltyp die Option Technischer Support aus.
5. Wählen Sie für Service AWS Control Tower.
6. Wählen Sie als Kategorie die Option General Guidance aus.
7. Geben Sie in der Betreffzeile den folgenden Satz ein:

   ```
   Allow retention of account-level trails during Landing Zone update
   ```
8. Geben Sie im Feld Beschreibung die folgenden Details ein:
   - Ihre AWS Management-Kontonummer
   - Die ausgewählte Heimatregion für Ihre AWS Control Tower Tower-Umgebung
9. Füllen Sie alle anderen erforderlichen Felder im Formular für Support-Anfragen aus.
10. Wählen Sie Senden, um den Supportfall zu erstellen.

Nachdem Sie das Ticket eingereicht haben, überprüft der AWS Support Ihre Anfrage und fügt Ihr Konto gegebenenfalls der Zulassungsliste hinzu. Weitere Anweisungen und eine Bestätigung erhalten Sie über den Kommunikationskanal für Support-Anfragen.

> **Note**
>
> Um den Trail auf Kontoebene zu löschen, nachdem er auf die Zulassungsliste gesetzt wurde, verwenden Sie das Verwaltungskonto, um das CloudFormation Stack-Set oder eine bestimmte Stack-Instance zu löschen. Alle Ressourcen im Stack werden gelöscht.

Beheben Sie Abweichungen mit Reset und Re-register

Abweichungen treten häufig auf, wenn Sie und Ihre Organisationsmitglieder die landing zone nutzen.

Die Drifterkennung erfolgt in AWS Control Tower automatisch. Automatisierte Scans Ihrer SCPs helfen Ihnen dabei, Ressourcen zu identifizieren, die Änderungen oder Konfigurationsupdates benötigen, um die Abweichung zu beheben.

Um viele Arten von Abweichungen zu beheben, wählen Sie in der Konsole auf der Seite mit den Landingzone-Einstellungen die Option Zurücksetzen aus. Außerdem können Sie einige Arten von Abweichungen beheben, indem Sie in der Konsole Re-registereine Organisationseinheit auswählen. Bei Steuerelementen können Sie Abweichungen programmgesteuert beheben, indem Sie die ResetEnabledControlAPI aufrufen. Weitere Informationen zu Drifttypen und deren Behebung finden Sie unter Arten von Abweichungen in der Unternehmensführung und. Abweichungen im AWS Control Tower erkennen und beheben

Ein Sonderfall der Driftauflösung tritt bei Rollendrift auf. Wenn eine erforderliche Rolle nicht verfügbar ist, zeigt die Konsole eine Warnseite und einige Anweisungen zur Wiederherstellung der Rolle an. Ihre landing zone ist nicht verfügbar, bis der Rollenwechsel behoben ist. Dieser Drift-Reset ist nicht dasselbe wie ein vollständiger Landezone-Reset. Weitere Informationen finden Sie im Abschnitt Erforderliche Rollen nicht löschenArten von Abweichungen, die sofort behoben werden müssen.

> **Wenn Sie Maßnahmen ergreifen, um Drift in einer landing zone Zone-Version zu beheben, hängt das Verhalten von Ihrer aktuellen Version ab.**
>
> - Wenn Sie die Landezone-Version 3.1 oder höher verwenden, können Sie „Aktualisieren“ wählen, um Ihre Landezonenkonfiguration zu ändern, ohne die Versionen zu aktualisieren, oder „Zurücksetzen“ wählen, um Ihre gespeicherten Konfigurationen erneut auf Ihre Drifting-Landing-Zone-Ressourcen anzuwenden. Die Drift wurde im Rahmen des Aktualisierungsprozesses behoben.

- Wenn Sie eine landing zone Zone-Version vor 3.1 verwenden, können Sie Reset nicht wählen. Sie müssen Update wählen und Ihre landing zone auf mindestens Version 3.1 aktualisieren.

Konten mithilfe von Automatisierung bereitstellen und aktualisieren

> **Note**
>
> Die Bereitstellung, Aktualisierung und Anpassung eines einzelnen Kontos muss auf eine Organisationseinheit (OU) abzielen, für die AWSControlTowerBaseline diese Option aktiviert ist. Wenn in einer Organisationseinheit das nicht AWSControlTowerBaseline aktiviert ist, können Sie die automatische Kontoregistrierung aktivieren oder ResetEnabledControl APIs auf ResetEnabledBaseline EnabledBaselines und EnabledControls auf dieser Organisationseinheit verwenden, um Konten zu registrieren. Einzelheiten zu finden Sie unter:. AWSControlTowerBaseline Basistypen, die auf OU-Ebene gelten

Sie können einzelne Konten in AWS Control Tower mit verschiedenen Methoden bereitstellen oder aktualisieren:

- Sie können Konten mit AWS Control Tower Account Factory for Terraform (AFT) bereitstellen und anpassen. Weitere Informationen finden Sie unter Überblick über AWS Control Tower Account Factory für Terraform (AFT).
- Sie können Konten mit Anpassungen für AWS Control Tower (cFCT) aktualisieren. Weitere Informationen finden Sie unter Übersicht über Anpassungen für AWS Control Tower (cFCT).
- Skriptautomatisierung: Wenn Sie lieber einen API-Ansatz verwenden, können Sie Konten mithilfe des API-Frameworks von Service Catalog aktualisieren und AWS CLI die Konten in einem Batch-Prozess aktualisieren. Sie würden die `UpdateProvisionedProduct`API von Service Catalog für jedes Konto aufrufen. Sie können ein Skript schreiben, um die Konten nacheinander mit dieser API zu aktualisieren. Weitere Informationen zu diesem Ansatz beim Hinzufügen von Regionen für die Verwaltung finden Sie im Blogbeitrag Enabling guardrails in new AWS Regions.

  Sie können bis zu fünf (5) Konten gleichzeitig aktualisieren. Sie müssen warten, bis mindestens eine Kontoaktualisierung erfolgreich war, bevor Sie mit der nächsten Kontoaktualisierung beginnen. Daher kann das Verfahren bei einer großen Anzahl von Konten lange dauern. Es ist jedoch nicht

kompliziert. Weitere Informationen zu diesem Ansatz finden Sie unter Automatisieren Sie die Kontobereitstellung in AWS Control Tower mithilfe von Service Catalog-APIs.

> **Video-Anleitung**
>
> Das Video-Anleitung ist für die automatische Kontobereitstellung mit einem Skript konzipiert. Die Schritte gelten jedoch auch für die Kontoaktualisierung. Verwenden Sie die `UpdateProvisionedProduct` API anstelle der `ProvisionProduct` API.

Ein weiterer Schritt der Automatisierung per Skript besteht darin, den Status Erfolgreich des AWS Control Tower `UpdateLandingZone` Tower-Lifecycle-Ereignisses zu überprüfen. Verwenden Sie es als Auslöser, um mit der Aktualisierung einzelner Konten zu beginnen, wie im Video beschrieben. Ein Lebenszyklusereignis markiert den Abschluss einer Abfolge von Aktivitäten. Das Eintreten dieses Ereignisses bedeutet also, dass ein Landingzone-Update abgeschlossen ist. Die Aktualisierung der Landing Zone muss vor Beginn der Kontoaktualisierung abgeschlossen sein. Weitere Informationen zum Arbeiten mit Lebenszyklus-Ereignissen finden Sie unter Lebenszyklus-Ereignisse.

Lesen Sie auch:

- Verwenden Sie AWS CloudShell um mit zu arbeiten AWS Control Tower.
- Automatisieren Sie Aufgaben im AWS Control Tower.

Automatisieren Sie Aufgaben im AWS Control Tower

Viele Kunden ziehen es vor, Aufgaben im AWS Control Tower zu automatisieren, z. B. die Kontobereitstellung, die Kontrollzuweisung und die Prüfung. Sie können diese automatisierten Aktionen mit folgenden Aufrufen einrichten:

- AWS Service Catalog APIs
- AWS Organizations APIs
- APIs für den AWS Control Tower
- die AWS CLI
- Ereignisse im Lebenszyklus

Die Zusätzliche Informationen und Links Seite enthält Links zu vielen hervorragenden technischen Blogbeiträgen, die Ihnen helfen können, Aufgaben in AWS Control Tower zu automatisieren.
Die folgenden Abschnitte enthalten Links zu Bereichen in diesem AWS Control Tower-Benutzerhandbuch, die Sie bei der Automatisierung von Aufgaben unterstützen können.

Automatisierung von Kontrollaufgaben

Sie können Aufgaben im Zusammenhang mit dem Anwenden und Entfernen von Kontrollen (auch als Leitplanken bezeichnet) über die AWS Control Tower-API automatisieren. Einzelheiten finden Sie in der AWS Control Tower API-Referenz.

Weitere Informationen zur Durchführung von Kontrolloperationen mit AWS Control Tower-APIs finden Sie im Blogbeitrag AWS Control Tower veröffentlicht API, vordefinierte Kontrollen für Ihre Organisationseinheiten.

Automatisierung von Aufgaben in der Landezone

Die AWS Control Tower-APIs für die Landezone helfen Ihnen bei der Automatisierung bestimmter Aufgaben im Zusammenhang mit Ihrer Landezone. Einzelheiten finden Sie in der API-Referenz für AWS Control Tower.

Automatisieren der OU-Registrierung

Die grundlegenden APIs von AWS Control Tower helfen Ihnen bei der Automatisierung bestimmter Aufgaben, wie z. B. der Registrierung einer OU. Einzelheiten finden Sie in der API-Referenz für AWS Control Tower.

Automatisierte Kontoschließung

Sie können die Schließung von AWS Control Tower-Mitgliedskonten mit einer AWS Organizations API automatisieren. Weitere Informationen finden Sie unter Schließen Sie ein AWS Control Tower-Mitgliedskonto über AWS Organizations.

Automatisierte Kontobereitstellung und Aktualisierung

Mit AWS Control Tower Account Factory Customization (AFC) können Sie Konten von der AWS Control Tower-Konsole aus erstellen. Dabei stehen benutzerdefinierte CloudFormation Vorlagen zur Verfügung, die wir als Blueprints bezeichnen. Dieser Prozess ist insofern automatisiert, als Sie nach der Einrichtung eines einzelnen Blueprints wiederholt neue Konten erstellen und Konten aktualisieren können, ohne die Pipelines verwalten zu müssen.

AWS Control Tower Account Factory for Terraform (AFT) folgt einem GitOps Modell zur Automatisierung der Prozesse der Kontobereitstellung und Kontoaktualisierung in AWS Control Tower. Weitere Informationen finden Sie unter Bereitstellung von Konten mit AWS Control Tower Account Factory für Terraform (AFT).

Anpassungen für den AWS Control Tower (cFCT) helfen Ihnen dabei, Ihre AWS Control Tower-Landezone anzupassen und stets auf dem neuesten Stand zu bleiben. AWS Anpassungen werden mithilfe von AWS CloudFormation Vorlagen, Service Control Policies (SCPs) und Resource Control Policies (RCPs) implementiert. Weitere Informationen finden Sie unter Übersicht über Anpassungen für AWS Control Tower (cFCT).

Weitere Informationen und ein Video zur automatisierten Kontobereitstellung finden Sie unter Exemplarische Vorgehensweise: Automatisierte Kontobereitstellung in AWS Control Tower und Automatisierte Bereitstellung mit IAM-Rollen.

Siehe auch Konten per Skript aktualisieren.

Programmatische Prüfung von Konten

Weitere Informationen zur programmgesteuerten Prüfung von Konten finden Sie unter Programmatische Rollen und Vertrauensbeziehungen für das AWS Control Tower-Prüfkonto.

Automatisierung anderer Aufgaben

Informationen darüber, wie Sie bestimmte AWS Control Tower-Servicekontingente mit einer automatisierten Anforderungsmethode erhöhen können, finden Sie in diesem Video: Automatisieren Sie die Erhöhung des Servicelimits.

Technische Blogs, die Anwendungsfälle von Automatisierung und Integration behandeln, finden Sie unter Automatisierung und Integration.

Zwei Open-Source-Beispiele sind unter verfügbar GitHub , um Ihnen bei bestimmten Automatisierungsaufgaben im Zusammenhang mit Sicherheit zu helfen.

- Das Beispiel aws-control-tower-org-setup-sample zeigt, wie Sie die Einrichtung des Audit-Kontos als delegierter Administrator für sicherheitsrelevante Dienste automatisieren können.
- Das Beispiel aws-control-tower-account-setup-using-step-functions zeigt, wie bewährte Sicherheitsmethoden bei der Bereitstellung und Konfiguration neuer Konten mithilfe von Step Functions automatisiert werden können. Dieses Beispiel umfasst das Hinzufügen von Principals zu Portfolios, die von der Organisation gemeinsam genutzt werden, und das automatische Zuordnen organisationsweiter IAM Identity Center-Gruppen zu neuen Konten. AWS Service Catalog AWS Es zeigt auch, wie die Standard-VPC in jeder Region gelöscht wird.

Die AWS Security Reference Architecture umfasst Codebeispiele für die Automatisierung von Aufgaben im Zusammenhang mit AWS Control Tower. Weitere Informationen finden Sie auf den Seiten mit AWS präskriptiven Anleitungen und im zugehörigen Repository. GitHub

Informationen zur Verwendung von AWS Control Tower mit einem AWS Service AWS CloudShell, der die Arbeit in der AWS CLI erleichtert, finden Sie unter AWS CloudShell und in der AWS CLI.

Da AWS Control Tower eine Orchestrierungsebene für ist AWS Organizations, sind viele andere AWS Dienste über APIs und die AWS CLI verfügbar. Weitere Informationen finden Sie unter Verwandte AWS Dienste.

Sie können die Automatisierung erweitern, indem Sie die vom AWS Control Tower ausgehenden Lebenszyklusereignisse verwenden. Diese Ereignisse können mithilfe einer EventBridge Amazon-Regel überwacht werden, die dann eine benutzerdefinierte Automatisierung auslösen kann, z. B. das Aufrufen einer AWS Lambda Funktion zum Anwenden von Tags, zur Konfiguration von Ressourcen oder zur Benachrichtigung von Teams, wenn bestimmte Konto- oder Kontrollereignisse in Ihrer Landezone auftreten.

Weitere Informationen zu Lebenszyklusereignissen finden Sie unter Lifecycle-Ereignisse im AWS Control Tower.

Verwenden Sie AWS CloudShell um mit zu arbeiten AWS Control Tower

AWS CloudShell ist ein AWS Dienst, der die Arbeit in der AWS CLI erleichtert — es handelt sich um eine browserbasierte, vorab authentifizierte Shell, die Sie direkt von der aus starten können. AWS-Managementkonsole Es ist nicht erforderlich, Befehlszeilentools herunterzuladen oder zu installieren. Sie können AWS CLI Befehle für AWS Control Tower und andere AWS Dienste von Ihrer bevorzugten Shell (Bash PowerShell oder Z-Shell) aus ausführen.

Wenn Sie AWS CloudShell von der aus starten AWS-Managementkonsole, sind die AWS Anmeldeinformationen, mit denen Sie sich bei der Konsole angemeldet haben, in einer neuen Shell-Sitzung verfügbar. Sie können die Eingabe Ihrer Anmeldeinformationen für die Konfiguration überspringen, wenn Sie mit AWS Control Tower und anderen AWS Diensten interagieren, und Sie verwenden AWS CLI Version 2, die in der Rechenumgebung der Shell vorinstalliert ist. Sie sind vorab authentifiziert mit. AWS CloudShell

Besorgen Sie sich IAM-Berechtigungen für AWS CloudShell

AWS Identity and Access Management stellt Ressourcen zur Zugriffsverwaltung bereit, mit denen Administratoren IAM-Benutzern und IAM Identity Center-Benutzern Berechtigungen für den Zugriff auf gewähren können. AWS CloudShell

Der schnellste Weg für einen Administrator, Benutzern Zugriff zu gewähren, ist eine AWS verwaltete Richtlinie. Bei einer von AWS verwalteten Richtlinie handelt es sich um eine eigenständige Richtlinie, die von AWS erstellt und verwaltet wird. Das folgende AWS verwaltete Richtlinienformular CloudShell kann an IAM-Identitäten angehängt werden:

- `AWSCloudShellFullAccess`: Erteilt die Erlaubnis zur Nutzung AWS CloudShell mit vollem Zugriff auf alle Funktionen.

Wenn Sie den Umfang der Aktionen einschränken möchten, die ein IAM-Benutzer oder IAM Identity Center-Benutzer ausführen kann AWS CloudShell, können Sie eine benutzerdefinierte Richtlinie erstellen, die die `AWSCloudShellFullAccess` verwaltete Richtlinie als Vorlage verwendet. Weitere Informationen zum Einschränken der Aktionen, die Benutzern in zur Verfügung stehen CloudShell, finden Sie im Benutzerhandbuch unter Verwaltung des AWS CloudShell Zugriffs und der AWS CloudShell Nutzung mit IAM-Richtlinien.

> **Note**
>
> Für Ihre IAM-Identität ist außerdem eine Richtlinie erforderlich, die Ihnen die Genehmigung erteilt, Anrufe an zu tätigen. AWS Control Tower Weitere Informationen finden Sie unter Für die Verwendung der AWS Control Tower Konsole erforderliche Berechtigungen.

Starten AWS CloudShell

Von dort aus können Sie starten AWS-Managementkonsole, CloudShell indem Sie die folgenden Optionen in der Navigationsleiste auswählen:

- Wählen Sie das CloudShell Symbol aus.
- Beginnen Sie mit der Eingabe von „Cloudshell“ in das Suchfeld und wählen Sie dann die CloudShell Option.

Jetzt, wo Sie angefangen haben CloudShell, können Sie alle AWS CLI Befehle eingeben, mit AWS Control Tower denen Sie arbeiten möchten. Sie können beispielsweise Ihren AWS Config Status überprüfen.

Interagiere mit AWS Control Tower durch AWS CloudShell

Nach dem Start AWS CloudShell von können Sie sofort mit der Interaktion über die AWS Control Tower Befehlszeilenschnittstelle beginnen. AWS-Managementkonsole AWS CLI Befehle funktionieren wie gewohnt in CloudShell.

> **Note**
>
> Wenn Sie AWS CLI in verwenden AWS CloudShell, müssen Sie keine zusätzlichen Ressourcen herunterladen oder installieren. Sie sind bereits in der Shell authentifiziert, sodass Sie keine Anmeldeinformationen konfigurieren müssen, bevor Sie Anrufe tätigen.

Verwenden Sie AWS CloudShell um bei der Einrichtung zu helfen AWS Control Tower

Bevor Sie diese Verfahren ausführen können, müssen Sie, sofern nicht anders angegeben, AWS-Managementkonsole in der Heimatregion Ihrer Landezone angemeldet sein. Sie müssen außerdem

als IAM Identity Center-Benutzer oder IAM-Benutzer mit Administratorberechtigungen für das Verwaltungskonto angemeldet sein, das Ihre Landing Zone enthält.

1. So können Sie AWS Config CLI-Befehle verwenden, AWS CloudShell um den Status Ihres Konfigurationsrekorders und Ihres Bereitstellungskanals zu ermitteln, bevor Sie mit der Konfiguration Ihrer AWS Control Tower Landing Zone beginnen.

   Beispiel: Überprüfen Sie Ihren AWS Config Status

   Befehle anzeigen:

   - `aws configservice describe-delivery-channels`
   - `aws configservice describe-delivery-channel-status`
   - `aws configservice describe-configuration-recorders`
   - Die normale Antwort ist so etwas wie `"name": "default"`

2. Wenn Sie bereits einen AWS Config Rekorder oder Übertragungskanal haben, den Sie löschen müssen, bevor Sie Ihre AWS Control Tower Landezone einrichten, können Sie folgende Befehle eingeben:

   Beispiel: Verwalte deine bereits vorhandenen Ressourcen AWS Config

   Befehle löschen:

   - `aws configservice stop-configuration-recorder --configuration-recorder-name` *`NAME-FROM-DESCRIBE-OUTPUT`*
   - `aws configservice delete-delivery-channel --delivery-channel-name` *`NAME-FROM-DESCRIBE-OUTPUT`*
   - `aws configservice delete-configuration-recorder --configuration-recorder-name` *`NAME-FROM-DESCRIBE-OUTPUT`*

   > **Important**
   >
   > Löschen Sie nicht die AWS Control Tower Ressourcen für AWS Config. Der Verlust dieser Ressourcen kann dazu führen AWS Control Tower , dass sie in einen inkonsistenten Zustand übergehen.

Weitere Informationen finden Sie auf der AWS Config Dokumentation

- Den Configuration Recorder (AWS CLI) verwalten
- Verwalten des Übermittlungskanals

3. Dieses Beispiel zeigt AWS CLI-Befehle, von denen aus Sie eingeben würden AWS CloudShell , um den vertrauenswürdigen Zugriff zu aktivieren oder zu deaktivieren AWS Organizations. Da AWS Control Tower Sie den vertrauenswürdigen Zugriff nicht aktivieren oder deaktivieren müssen AWS Organizations, ist dies nur ein Beispiel. Möglicherweise müssen Sie jedoch den vertrauenswürdigen Zugriff für andere AWS Dienste aktivieren oder deaktivieren, wenn Sie Aktionen in automatisieren oder anpassen. AWS Control Tower

   Beispiel: Den Zugriff auf vertrauenswürdige Dienste aktivieren oder deaktivieren

   - `aws organizations enable-aws-service-access`
   - `aws organizations disable-aws-service-access`

Beispiel: Erstellen Sie einen Amazon S3-Bucket mit AWS CloudShell

Im folgenden Beispiel können Sie es verwenden, AWS CloudShell um einen Amazon S3-Bucket zu erstellen und dann die PutObject Methode zu verwenden, um eine Codedatei als Objekt in diesem Bucket hinzuzufügen.

1. Um einen Bucket in einer bestimmten AWS Region zu erstellen, geben Sie den folgenden Befehl in die CloudShell Befehlszeile ein:

   ```
   aws s3api create-bucket --bucket insert-unique-bucket-name-here --region us-east-1
   ```

   Wenn der Aufruf erfolgreich ist, zeigt die Befehlszeile eine Antwort des Services an, die der folgenden Ausgabe ähnelt:

   ```
   {
       "Location": "/insert-unique-bucket-name-here"
   }
   ```

> **Note**
>
> Wenn Sie die Regeln für die Benennung von Buckets nicht einhalten (z. B. nur Kleinbuchstaben verwenden), wird der folgende Fehler angezeigt: Beim Aufrufen der CreateBucket Operation ist ein Fehler aufgetreten (InvalidBucketName): Der angegebene Bucket ist nicht gültig.

2. Um eine Datei hochzuladen und sie dem Bucket, der gerade erstellt wurde, als Objekt hinzuzufügen, rufen Sie die PutObject Methode auf:

```
aws s3api put-object --bucket insert-unique-bucket-name-here --key add_prog --body
 add_prog.py
```

Wenn das Objekt erfolgreich in den Amazon S3-Bucket hochgeladen wurde, zeigt die Befehlszeile eine Antwort des Dienstes an, die der folgenden Ausgabe ähnelt:

```
{
            "ETag": "\"ab123c1:w:wad4a567d8bfd9a1234ebeea56\""}
```

Das `ETag` ist der Hash des Objekts, das gespeichert wurde. Er kann verwendet werden, um die Integrität des auf Amazon S3 hochgeladenen Objekts zu überprüfen.

Create AWS Control Tower Ressourcen mit AWS CloudFormation

AWS Control Tower ist in einen Service integriert AWS CloudFormation, der Ihnen hilft, Ihre AWS Ressourcen zu modellieren und einzurichten, sodass Sie weniger Zeit mit der Erstellung und Verwaltung Ihrer Ressourcen und Infrastruktur verbringen müssen. Sie erstellen eine Vorlage, die alle benötigten AWS Ressourcen beschreibt, z. B. `AWS::ControlTower::EnabledControl` für Steuerelemente. CloudFormation stellt diese Ressourcen für Sie bereit und konfiguriert sie.

Wenn Sie sie verwenden CloudFormation, können Sie Ihre Vorlage wiederverwenden, um Ihre AWS Control Tower Ressourcen konsistent und wiederholt einzurichten. Beschreiben Sie Ihre Ressourcen einmal und stellen Sie dann dieselben Ressourcen immer wieder in mehreren AWS-Konten und Regionen bereit.

AWS Control Tower und CloudFormation Vorlagen

Um Ressourcen für und damit verbundene Dienste bereitzustellen AWS Control Tower und zu konfigurieren, müssen Sie sich mit CloudFormation Vorlagen auskennen. Vorlagen sind formatierte Textdateien in JSON oder YAML. Diese Vorlagen beschreiben die Ressourcen, die Sie in Ihren CloudFormation Stacks bereitstellen möchten. Wenn Sie mit JSON oder YAML nicht vertraut sind, können Sie AWS Infrastructure Composer verwenden, um Ihnen den Einstieg in Vorlagen zu erleichtern. CloudFormation Weitere Informationen finden Sie unter Was ist AWS Infrastructure Composer? im AWS Infrastructure Composer-Benutzerhandbuch.

AWS Control Tower unterstützt das Erstellen von `AWS::ControlTower::EnabledControl` (Kontrollressourcen), `AWS::ControlTower::LandingZone` (Landezonen) und `AWS::ControlTower::EnabledBaseline` (Basislinien) in. CloudFormation Weitere Informationen, einschließlich Beispielen für JSON- und YAML-Vorlagen für diese Ressourcentypen, finden Sie AWS Control Tower im AWS CloudFormation Benutzerhandbuch.

> **Note**
>
> Das Limit für `EnableControl` und `DisableControl` Aktualisierungen AWS Control Tower liegt bei 100 gleichzeitigen Vorgängen.

Einige AWS Control Tower Beispiele für die CLI und die Konsole finden Sie unter Steuerelemente aktivieren mit CloudFormation.

Erfahren Sie mehr über CloudFormation

Weitere Informationen CloudFormation dazu finden Sie in den folgenden Ressourcen:

- AWS CloudFormation
- AWS CloudFormation Benutzerhandbuch
- CloudFormation API Referenz
- AWS CloudFormation Benutzerhandbuch für die Befehlszeilenschnittstelle

Passen Sie Ihre AWS Control Tower-Landezone an

Bestimmte Aspekte Ihrer AWS Control Tower-Landezone sind in der Konsole konfigurierbar, z. B. die Auswahl von Regionen und optionale Steuerungen. Andere Änderungen können automatisiert außerhalb der Konsole vorgenommen werden.

Beispielsweise können Sie mit der Funktion Anpassungen für den AWS Control Tower, einem GitOps-style Anpassungsframework, das mit AWS CloudFormation Vorlagen und AWS Control Tower-Lebenszyklusereignissen funktioniert, umfangreichere Anpassungen Ihrer Landezone erstellen.

Passen Sie es von der AWS Control Tower-Konsole aus an

Um diese Anpassungen an Ihrer Landing Zone vorzunehmen, folgen Sie den Anweisungen auf der AWS Control Tower-Konsole.

Wählen Sie bei der Einrichtung benutzerdefinierte Namen aus

- Sie können bei der Einrichtung die Namen Ihrer Organisationseinheiten auf oberster Ebene auswählen. Sie können Ihre Organisationseinheiten jederzeit mithilfe der AWS Organizations Konsole umbenennen. Wenn Sie jedoch Änderungen an Ihren Organisationseinheiten vornehmen, AWS Organizations kann dies zu reparierbaren Abweichungen führen.
- Sie können die Namen Ihrer gemeinsam genutzten Audit - und Log Archive-Konten auswählen, aber Sie können die Namen nach der Einrichtung nicht mehr ändern. (Dies ist eine einmalige Auswahl.)

> **Tipp**
>
> Denken Sie daran, dass das Umbenennen einer Organisationseinheit in AWS Organizations das entsprechende bereitgestellte Produkt in Account Factory nicht aktualisiert. Um das bereitgestellte Produkt automatisch zu aktualisieren (und Abweichungen zu vermeiden), müssen Sie den OU-Vorgang über AWS Control Tower ausführen, einschließlich des Erstellens, Löschens oder erneuten Registrierens einer Organisationseinheit.

Select AWS Regionen

- Sie können Ihre Landezone anpassen, indem Sie bestimmte AWS Regionen für die Steuerung auswählen. Folgen Sie den Schritten in der AWS Control Tower-Konsole.
- Wenn Sie Ihre Landezone aktualisieren, können Sie AWS Regionen für die Verwaltung auswählen und abwählen.
- Du kannst die Steuerung „Region verweigern“ auf „Aktiviert“ oder „Nicht aktiviert“ setzen und den Benutzerzugriff auf die meisten AWS Dienste in Regionen ohne Kontrolle kontrollieren. AWS

Informationen darüber, AWS-Regionen wo CfCT Einsatzbeschränkungen hat, finden Sie unter. Einschränkungen bei der Steuerung

Passen Sie an, indem Sie optionale Steuerelemente hinzufügen

- Dringend empfohlene und optionale Steuerungen sind optional, was bedeutet, dass Sie die Durchsetzungsstufe für Ihre Landezone anpassen können, indem Sie auswählen, welche aktiviert werden sollen. Optionale Steuerungen sind standardmäßig nicht aktiviert.
- Mit den optionalen Steuerelementen zum Speichern von Daten können Sie die Regionen, in denen Sie Ihre Daten speichern, anpassen und den Zugriff darauf gewähren.
- Die optionalen Steuerelemente, die Teil des integrierten Security Hub CSPM-Standards sind, ermöglichen es Ihnen, Ihre AWS Control Tower-Umgebung auf Sicherheitsrisiken zu überprüfen.
- Mit den optionalen proaktiven Kontrollen können Sie Ihre CloudFormation Ressourcen überprüfen, bevor sie bereitgestellt werden, um sicherzustellen, dass die neuen Ressourcen den Kontrollzielen Ihrer Umgebung entsprechen.

Passen Sie Ihre an AWS CloudTrail Trails

- Wenn Sie Ihre Landezone auf Version 3.0 oder höher aktualisieren, können Sie wählen, ob Sie die vom AWS Control Tower verwalteten CloudTrail Trails auf Organisationsebene aktivieren oder deaktivieren möchten. Sie können diese Auswahl jederzeit ändern, wenn Sie Ihre Landezone aktualisieren. AWS Control Tower erstellt in Ihrem Verwaltungskonto einen Pfad auf Organisationsebene, und dieser Pfad wechselt je nach Ihrer Wahl in den Status „Aktiv“ oder „Inaktiv“. Landing Zone 3.0 unterstützt keine CloudTrail Trails auf Kontoebene. Wenn Sie diese jedoch benötigen, können Sie Ihre eigenen Trails konfigurieren und verwalten. Für doppelte Trails können zusätzliche Kosten anfallen.

Erstelle benutzerdefinierte Mitgliedskonten in der Konsole

- Sie können benutzerdefinierte AWS Control Tower-Mitgliedskonten erstellen und bestehende Mitgliedskonten von der AWS Control Tower-Konsole aus aktualisieren, um Anpassungen hinzuzufügen. Weitere Informationen finden Sie unter Passen Sie Konten mit Account Factory Customization (AFC) an.

Automatisieren Sie Anpassungen außerhalb der AWS Control Tower-Konsole

Einige Anpassungen sind nicht über die AWS Control Tower-Konsole verfügbar, können aber auf andere Weise implementiert werden. Beispiel:

- Sie können Konten während der Bereitstellung in einem GitOps-style Workflow mit Account Factory for Terraform (AFT) anpassen.

  AFT wird mit einem Terraform-Modul bereitgestellt, das im AFT-Repository verfügbar ist. https://github.com/aws-ia/terraform-aws-control_tower_account_factory/tree/main
- Sie können Ihre AWS Control Tower-Landezone mit Anpassungen für den AWS Control Tower (cFCT) anpassen. Dabei handelt es sich um ein Funktionspaket, das auf AWS CloudFormation Vorlagen und Service Control Policies (SCPs) basiert. Sie können die benutzerdefinierten Vorlagen und Richtlinien für einzelne Konten und Organisationseinheiten (OUs) innerhalb Ihrer Organisation bereitstellen.

  Der Quellcode für cFCT ist in einem GitHub Repository verfügbar.
- Sie können Ihre AWS Control Tower-Landezone anpassen, wenn der Landing Zone Accelerator (LZA) aktiviert ist. AWS Die LZA-Lösung ist so konzipiert, dass sie sich an AWS bewährten Verfahren orientiert und mehreren globalen Compliance-Frameworks entspricht. Wir empfehlen, den AWS Control Tower als grundlegende Landezone bereitzustellen und dann die Funktionen der Landezone bei Bedarf mit LZA zu erweitern. Weitere Informationen finden Sie unter AWS Control Tower und Landing Zone Accelerator.

AWS-Kontrollturm und Landezonenbeschleuniger

In diesem Abschnitt werden die Vorteile der Zusammenarbeit mit dem AWS Control Tower und der Landing Zone Accelerator (LZA) -Lösung beschrieben.

Sie können Ihre AWS Control Tower-Landezone anpassen, wenn der Landing Zone Accelerator (LZA) aktiviert ist. AWS

LZA ist eine Lösung, die eine Reihe grundlegender Funktionen bereitstellt, die auf AWS Best Practices und mehrere globale Compliance-Frameworks abgestimmt sind, um Sie bei der Verwaltung und Steuerung einer Umgebung mit mehreren Konten zu unterstützen. LZA wurde mit dem AWS Cloud Development Kit (CDK) erstellt.

LZA richtet automatisch eine Cloud-Umgebung ein, die für das Hosten sicherer Workloads geeignet ist. Diese Lösung kann überall eingesetzt werden AWS-Regionen, um Ihnen zu helfen, die Konsistenz von Betrieb und Verwaltung aufrechtzuerhalten. Die LZA-Lösung ist so konzipiert, dass sie sich an AWS Best Practices orientiert und mehreren globalen Compliance-Frameworks entspricht.

Wir empfehlen Ihnen, den AWS Control Tower als Ihre grundlegende Landezone bereitzustellen und dann Ihre Landezonen-Funktionen bei Bedarf mit LZA zu erweitern. Die Kombination aus LZA und AWS Control Tower bietet eine umfassende, codefreie Lösung, mit der Sie eine Umgebung mit mehreren Konten verwalten und steuern können. Sie wurde entwickelt, um stark regulierte Workloads und komplexe Compliance-Anforderungen zu unterstützen. Zusammen helfen Ihnen der AWS Control Tower und der Landing Zone Accelerator dabei, die Plattformbereitschaft sicherzustellen, einschließlich Sicherheits-, Compliance- und Betriebsfunktionen.

Der Quellcode für LZA ist in einem GitHub Repository verfügbar.

Weitere Informationen zur Kombination von LZA und AWS Control Tower finden Sie im LZA-Implementierungsleitfaden.

Vorteile von Anpassungen für AWS Control Tower (cFCT)

Das Funktionspaket, das wir als Anpassungen für den AWS Control Tower (cFCT) bezeichnen, hilft Ihnen dabei, umfangreichere Anpassungen für Ihre Landing Zone zu erstellen, als Sie es in der AWS Control Tower-Konsole tun können. Es bietet einen automatisierten Prozess GitOps-style. Sie können Ihre Landezone an Ihre Geschäftsanforderungen anpassen.

Bei diesem Prozess zur Anpassung der Infrastruktur als Code werden AWS CloudFormation Vorlagen mit AWS Service Control Policies (SCPs), Resource Control Policies (RCPs) und AWS Control Tower-Lifecycle-Ereignissen integriert, sodass Ihre Ressourcenbereitstellungen mit Ihrer Landezone synchronisiert bleiben. Wenn Sie beispielsweise ein neues Konto bei Account Factory erstellen, können die mit dem Konto und der OU verknüpften Ressourcen automatisch bereitgestellt werden.

> **Note**
>
> Im Gegensatz zu Account Factory und AFT ist cFCT nicht speziell für die Erstellung neuer Konten vorgesehen, sondern für die Anpassung von Konten und OUs in Ihrer Landing Zone durch den Einsatz von Ressourcen, die Sie angeben.

> **Note**
>
> Die in cFCT konfigurierte Zielorganisationseinheit (OU) muss im AWS Control Tower AWSControlTowerBaseline aktiviert sein. Einzelheiten finden Sie AWSControlTowerBaseline unter:Basistypen, die auf OU-Ebene gelten.

Vorteile

- Erweitern Sie eine maßgeschneiderte und sichere AWS Umgebung — Sie können Ihre AWS Control Tower-Umgebung mit mehreren Konten schneller erweitern und AWS bewährte Methoden in einen wiederholbaren Anpassungsworkflow integrieren.
- Instanziieren Sie Ihre Anforderungen — Sie können Ihre AWS Control Tower-Landing Zone an Ihre Geschäftsanforderungen anpassen, indem Sie die AWS CloudFormation Vorlagen und Servicekontrolle-Richtlinien verwenden, die Ihre politischen Absichten zum Ausdruck bringen.
- Automatisieren Sie mit AWS Control Tower-Lifecycle-Ereignissen weiter — Lifecycle-Ereignisse ermöglichen es Ihnen, Ressourcen auf der Grundlage des Abschlusses einer früheren Reihe von Ereignissen bereitzustellen. Sie können sich darauf verlassen, dass ein Lebenszyklusereignis Ihnen hilft, Ressourcen automatisch für Konten und Organisationseinheiten bereitzustellen.
- Erweitern Sie Ihre Netzwerkarchitektur — Sie können maßgeschneiderte Netzwerkarchitekturen bereitstellen, die Ihre Konnektivität verbessern und schützen, z. B. ein Transit-Gateway.

Weitere cFCT-Beispiele

- Ein Beispiel für einen Netzwerk-Anwendungsfall mit Anpassungen für AWS Control Tower (cFCT) finden Sie im AWS Architektur-Blogbeitrag Deploy consistent DNS with Service Catalog and AWS Control Tower Customizations.
- Ein konkretes Beispiel im Zusammenhang mit cFCT und Amazon GuardDuty ist im GitHub Repository verfügbar. `aws-samples`

- Zusätzliche Codebeispiele zu cFCT sind als Teil der AWS Security Reference Architecture im `aws-samples` Repository verfügbar. Viele dieser Beispiele enthalten `manifest.yaml` Beispieldateien in einem Verzeichnis mit dem Name`customizations_for_aws_control_tower`.

Weitere Informationen zur AWS Security Reference Architecture finden Sie auf den Seiten mit AWS präskriptiven Anleitungen.

Übersicht über Anpassungen für AWS Control Tower (cFCT)

Customizations for AWS Control Tower (cFCT) hilft Ihnen dabei, Ihre AWS Control Tower Tower-Landing landing zone individuell anzupassen und dabei stets die AWS bewährten Methoden einzuhalten. Anpassungen werden mit AWS CloudFormation Vorlagen, Service Control Policies (SCPs) und Resource Control Policies (RCPs) implementiert.

Diese cFCT-Funktion ist in die Lebenszyklusereignisse von AWS Control Tower integriert, sodass Ihre Ressourcenbereitstellungen mit Ihrer landing zone synchronisiert bleiben. Wenn beispielsweise ein neues Konto über Account Factory erstellt wird, werden alle mit dem Konto verknüpften Ressourcen automatisch bereitgestellt. Sie können die benutzerdefinierten Vorlagen und Richtlinien für einzelne Konten und Organisationseinheiten (OUs) innerhalb Ihrer Organisation bereitstellen.

> **Note**
>
> Die in CfCT konfigurierte Zielorganisationseinheit (OU) muss in AWS Control Tower AWSControlTowerBaseline aktiviert worden sein. Einzelheiten zu finden Sie AWSControlTowerBaseline unter:Basistypen, die auf OU-Ebene gelten.

Das folgende Video beschreibt bewährte Methoden für die Bereitstellung einer skalierbaren CfCT-Pipeline und allgemeine cFcT-Anpassungen.

Der folgende Abschnitt enthält architektonische Überlegungen und Konfigurationsschritte für die Bereitstellung von Anpassungen für AWS Control Tower (cFCT). Er enthält einen Link zu der AWS CloudFormationVorlage, mit der die erforderlichen AWS Services gemäß den AWS bewährten Methoden für Sicherheit und Verfügbarkeit gestartet, konfiguriert und ausgeführt werden.

Dieses Thema richtet sich an Architekten und Entwickler von IT-Infrastrukturen, die über praktische Erfahrung mit der Architektur in der AWS Cloud verfügen.

Informationen zu den neuesten Updates und Änderungen an Customizations for AWS Control Tower (cFCT) finden Sie in der CHANGELOG.md Datei im Repository. GitHub

Übersicht über die Architektur

Durch die Bereitstellung von CfCT wird die folgende Umgebung in der AWS Cloud mit einem Amazon S3 S3-Bucket als Konfigurationsquelle erstellt.

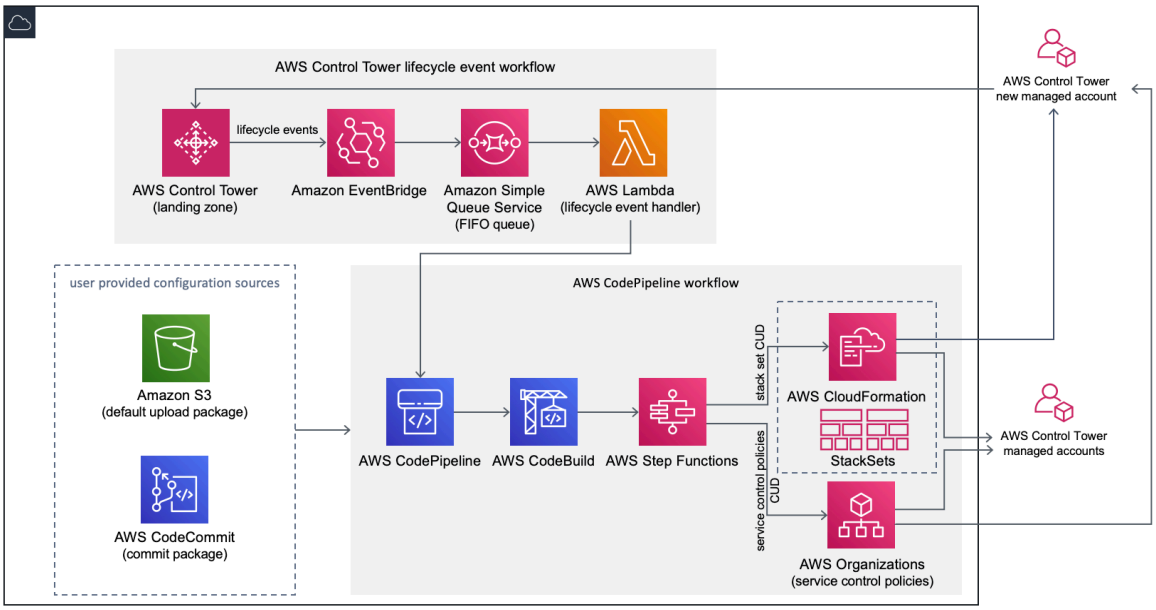

Abbildung 1: Anpassungen für die AWS Control Tower Tower-Architektur

CfCT enthält eine AWS CloudFormation Vorlage, die Sie in Ihrem AWS Control Tower Tower-Managementkonto bereitstellen. Die Vorlage startet alle Komponenten, die für die Erstellung der Workflows erforderlich sind, sodass Sie Ihre AWS Control Tower Tower-Landezone anpassen können.

> **Hinweis**
>
> CfCT muss in der AWS Control Tower Tower-Heimatregion und im AWS Control Tower Tower-Managementkonto bereitgestellt werden, da dort Ihre AWS Control Tower Tower-Landezone bereitgestellt wird. Informationen zur Einrichtung einer AWS Control Tower Tower-Landezone finden Sie unterErste Schritte.

Bei der Bereitstellung von CfCT werden die benutzerdefinierten Ressourcen mithilfe von Amazon Simple Storage Service (Amazon S3) verpackt und in die Code-Pipeline-Quelle hochgeladen.

Beim Upload werden automatisch die Zustandsmaschine für Service Control Policies (SCPs), die Zustandsmaschine für Resource Control Policies (RCPs) und die AWS CloudFormation StackSetsZustandsmaschine aufgerufen, um die SCPs und RCPs auf OU-Ebene oder Stack-Instances auf OU- oder Kontoebene bereitzustellen.

> **Hinweis**
>
> Standardmäßig erstellt CfCT einen Amazon S3 S3-Bucket zum Speichern der Pipeline-Quelle. Wenn Sie über ein vorhandenes AWS CodeCommit Repository verfügen, können Sie den Speicherort in ein CodeCommitRepository ändern. Weitere Informationen finden Sie unter Amazon S3 als Konfigurationsquelle einrichten.

CfCT stellt zwei Workflows bereit:

- ein Workflow AWS CodePipeline
- und ein AWS Control Tower Tower-Lifecycle-Event-Workflow.

Der AWS CodePipeline Arbeitsablauf

Der AWS CodePipeline Workflow konfiguriert AWS CodePipeline, AWS CodeBuildprojektiert und orchestriert AWS Step Functionsdie Verwaltung von AWS CloudFormation StackSets SCPs und RCPs in Ihrer Organisation.

Wenn Sie das Konfigurationspaket hochladen, ruft CfCT die Code-Pipeline auf, um vier Phasen auszuführen.

- Build Stage — validiert den Inhalt des Konfigurationspakets mithilfe von AWS CodeBuild.
- SCP Stage — ruft die Service Control Policy State Machine auf, die die AWS Organizations API aufruft, um SCPs zu erstellen.
- RCP Stage — ruft die Resource Control Policy State Machine auf, die die API aufruft, um RCPs zu erstellen. AWS Organizations
- CloudFormation Stage — ruft die Stackset-Zustandsmaschine auf, um die Ressourcen bereitzustellen, die in der Liste der Konten oder Organisationseinheiten angegeben sind, die Sie in der Manifestdatei angegeben haben.

In jeder Phase ruft die Code-Pipeline die Stack-Set-, SCP- und RCP-Schrittfunktionen auf, die benutzerdefinierte Stacksets, SCPs und RCPs für einzelne Zielkonten oder für eine gesamte Organisationseinheit bereitstellen.

> **Hinweis**
>
> Ausführliche Informationen zum Anpassen des Konfigurationspakets finden Sie unter. Leitfaden zur cFCT-Anpassung

Der Workflow für Lebenszyklusereignisse von AWS Control Tower

Wenn ein neues Konto in AWS Control Tower erstellt wird, kann ein Lebenszyklusereignis den AWS CodePipeline Workflow aufrufen. Sie können das Konfigurationspaket über diesen Workflow anpassen, der aus einer EventBridgeAmazon-Ereignisregel, einer First-in-First-Out-Warteschlange (FIFO) von Amazon Simple Queue Service (Amazon SQS) und einer Funktion besteht. AWS Lambda

Wenn die EventBridge Amazon-Ereignisregel ein entsprechendes Lebenszyklusereignis erkennt, leitet sie das Ereignis an die Amazon SQS-FIFO-Warteschlange weiter, ruft die AWS Lambda Funktion auf und ruft die Code-Pipeline auf, um die nachgelagerte Bereitstellung von Stack-Sets, SCPs und RCPs durchzuführen.

Cost (Kosten)

Die Kosten für die Ausführung von CfCT hängen von der Anzahl der AWS CodePipeline Läufe, der Dauer der AWS CodeBuild Läufe, der Anzahl und Dauer der AWS Lambda Funktionen und der Anzahl der veröffentlichten EventBridge Amazon-Ereignisse ab. Wenn Sie beispielsweise 100 Builds in einem Monat mit build.general1.small ausführen, wobei jeder Build fünf Minuten lang läuft, belaufen sich die ungefähren Kosten für die Ausführung von cFCT auf 3,00 USD pro Monat. Vollständige Informationen finden Sie auf der Webseite mit den Preisen für jeden Dienst, den Sie nutzen. AWS

Der Bucket und die AWS CodeCommit Git-based Repository-Ressourcen von Amazon Simple Storage Service (Amazon S3) werden nach dem Löschen der Vorlage beibehalten, um Ihre Konfigurationsinformationen zu schützen. Je nach der von Ihnen ausgewählten Option werden Ihnen Gebühren auf der Grundlage der im Amazon S3 S3-Bucket gespeicherten Datenmenge und der Anzahl der Git-Anfragen berechnet (gilt nicht für Amazon S3 S3-Ressourcen). Einzelheiten finden Sie unter Amazon S3 und AWS CodeCommitPreise.

Komponentendienste

Die folgenden AWS Services sind Bestandteile von Anpassungen für AWS Control Tower (cFCT).

AWS CodeCommit

Wenn Sie über ein vorhandenes AWS CodeCommit Repository verfügen, können Sie es als Alternative zu Amazon S3 als Quelle für Ihre Pipeline konfigurieren.

Basierend auf Ihren Eingaben in die CloudFormation Vorlage kann cFCT ein AWS CodeCommit Repository mit derselben Beispielkonfiguration erstellen, die im Abschnitt Amazon Simple Storage Service erklärt wird.

Um das AWS CodeCommit cFCT-Repository auf Ihren lokalen Computer zu klonen, müssen Sie Anmeldeinformationen erstellen, die Ihnen temporären Zugriff auf das Repository gewähren, wie im AWS CodeCommit Benutzerhandbuch beschrieben. Informationen zur Versionskompatibilität finden Sie unter Einrichten von. AWS CodeCommit

> **Note**
>
> Wenn Sie ihn noch nicht verwenden CodeCommit, besteht Ihre einzige Möglichkeit darin, den Amazon S3-Bucket als Speicherort für Ihr Konfigurationspaket einzurichten. CodeCommit ist nicht verfügbar, wenn Sie cFCT zum ersten Mal bereitstellen.

AWS CodePipeline

AWS CodePipeline validiert, testet und implementiert Änderungen auf der Grundlage von Aktualisierungen des Konfigurationspakets, die Sie entweder im standardmäßigen Amazon S3-Bucket oder im AWS CodeCommit Repository vornehmen. Weitere Informationen zur Konfigurationsquellensteuerung finden Sie unter Amazon S3 als Konfigurationsquelle verwenden. Die Pipeline umfasst Etappen zur Validierung und Verwaltung der Konfigurationsdateien und Vorlagen, Kernkonten, AWS Organizations Servicesteuerungsrichtlinien AWS CloudFormation StackSets usw. Weitere Informationen zu den Pipeline-Phasen finden Sie unter Leitfaden zur cFCT-Anpassung

AWS Key Management Service

CfCT erstellt einen AWS Key Management Service (AWS KMS) `CustomControlTowerKMSKey` -Verschlüsselungsschlüssel. Dieser Schlüssel wird verwendet, um Objekte im Amazon S3-Konfigurations-Bucket, in der Amazon SQS-Warteschlange und vertrauliche Parameter im AWS Systems Manager-Parameterspeicher zu verschlüsseln. Standardmäßig sind nur von cFCT bereitgestellte Rollen berechtigt, Verschlüsselungs- oder Entschlüsselungsvorgänge mit diesem Schlüssel durchzuführen. Für den Zugriff auf die `SecureString` Werte der Konfigurationsdatei, der FIFO-Warteschlange oder des Parameterspeichers müssen der Richtlinie Administratoren hinzugefügt werden. `CustomControlTowerKMSKey` Die automatische Schlüsselrotation ist standardmäßig aktiviert.

AWS Lambda

cFCT verwendet AWS Lambda Funktionen, um die Installationskomponenten während der Erstinstallation und Bereitstellung von AWS CloudFormation StackSets oder AWS Organizations SCPs während eines AWS Control Tower-Lifecycle-Ereignisses aufzurufen.

Amazon Simple Notification Service

cFCT kann während des Workflows Benachrichtigungen, wie z. B. die Genehmigung der Pipeline, zu Themen des Amazon Simple Notification Service (Amazon SNS) veröffentlichen. Amazon SNS wird nur gestartet, wenn Sie sich dafür entscheiden, Benachrichtigungen zur Pipeline-Genehmigung zu erhalten.

Amazon Simple Storage Service

Wenn Sie cFCT bereitstellen, erstellt cFCT einen Amazon Simple Storage Service (Amazon S3) -Bucket mit einem eindeutigen Namen:

Beispiel: Name des Amazon S3-Buckets

`custom-control-tower-configuration-`*`accountID`*`-`*`region`*

Der Bucket enthält eine Beispielkonfigurationsdatei mit dem Namen `_custom-control-tower-configuration.zip`

Beachten Sie den führenden Unterstrich im Dateinamen.

Diese ZIP-Datei enthält ein Beispielmanifest und die zugehörigen Beispielvorlagen, die die erforderliche Ordnerstruktur beschreiben. Diese Beispiele helfen Ihnen bei der Entwicklung eines Konfigurationspakets zur Anpassung Ihrer AWS Control Tower-Landezone. Das Beispielmanifest identifiziert die erforderlichen Konfigurationen für Stack-Sets und Service Control Policies (SCPs), die Sie bei der Implementierung Ihrer Anpassungen benötigen.

Sie können dieses Beispielkonfigurationspaket als Modell verwenden, um Ihr benutzerdefiniertes Paket zu entwickeln und hochzuladen, das die cFCT-Konfigurationspipeline automatisch auslöst.

Hinweise zum Anpassen der Konfigurationsdatei finden Sie unter. Leitfaden zur cFCT-Anpassung

Amazon Simple Queue Service

cFCT verwendet eine FIFO-Warteschlange von Amazon Simple Queue Service (Amazon SQS), um Lebenszyklusereignisse von Amazon zu erfassen. EventBridge Sie löst eine AWS Lambda Funktion aus, die zwei oder mehrere SCPs AWS CodePipeline aufruft. AWS CloudFormation StackSets Weitere Informationen zu SCPs finden Sie unter. AWS Organizations

AWS Step Functions

cFCT erstellt Step Functions zur Orchestrierung von Anpassungsbereitstellungen. Diese Step Functions übersetzen Konfigurationsdateien, um die Anpassungen nach Bedarf in allen Umgebungen bereitzustellen.

AWS Systems Manager Parameter Store

Der AWS Systems Manager Parameter Store speichert die cFCT-Konfigurationsparameter. Mit diesen Parametern können Sie verwandte Konfigurationsvorlagen integrieren. Sie können beispielsweise jedes Konto so konfigurieren, dass AWS CloudTrail Daten in einem zentralen Amazon S3-Bucket protokolliert werden. Außerdem bietet der Systems Manager Parameter Store einen zentralen Ort, an dem Administratoren cFCT-Eingaben und -Parameter einsehen können.

Überlegungen zur Bereitstellung

Stellen Sie sicher, dass Sie Customizations for AWS Control Tower (cFCT) in demselben Konto und derselben Region starten, in der Ihre AWS Control Tower Tower-Landezone bereitgestellt wird. Das heißt, Sie müssen sie im AWS Control Tower Tower-Verwaltungskonto in Ihrer AWS Control Tower Tower-Heimatregion bereitstellen. Standardmäßig erstellt CfCT das landing zone Zone-

Konfigurationspaket und führt es aus, indem es eine Konfigurationspipeline in diesem Konto und dieser Region einrichtet.

Bereiten Sie sich auf die Bereitstellung vor

Sie haben einige Optionen, wenn Sie Ihre CloudFormation Vorlage für die erste Bereitstellung vorbereiten. Sie können die Konfigurationsquelle auswählen und die manuelle Genehmigung von Pipeline-Bereitstellungen zulassen. In den nächsten beiden Abschnitten werden diese Optionen näher erläutert.

Wählen Sie Ihre Konfigurationsquelle

Standardmäßig erstellt die Vorlage einen Amazon Simple Storage Service (Amazon S3) -Bucket, in dem das Beispielkonfigurationspaket als `.zip` Datei mit dem Namen gespeichert wird`_custom-control-tower-configuration.zip`. Der Amazon S3 S3-Bucket ist versionsgesteuert, und Sie können das Konfigurationspaket nach Bedarf aktualisieren. Informationen zur Aktualisierung des Konfigurationspakets finden Sie unter Amazon S3 als Konfigurationsquelle verwenden.

> **Denken Sie daran, den Unterstrich zu entfernen**
>
> Der Dateiname des Beispielkonfigurationspakets beginnt mit einem Unterstrich (_), sodass er nicht automatisch initiiert AWS CodePipeline wird. Wenn Sie mit der Anpassung des Konfigurationspakets fertig sind, stellen Sie sicher, dass Sie das Paket `custom-control-tower-configuration.zip` ohne den Unterstrich (_) hochladen, um mit der Bereitstellung in zu beginnen. AWS CodePipeline

Wenn Sie über ein vorhandenes AWS CodeCommit Git-Repository verfügen, können Sie den Speicherort des Konfigurationspakets vom Amazon S3 S3-Bucket in ein AWS CodeCommit Git-Repository ändern. Wählen Sie dazu die `CodeCommit` Option im CloudFormation Parameter aus.

> **Zippen oder nicht komprimieren?**
>
> Wenn Sie den Standard-S3-Bucket verwenden, stellen Sie sicher, dass das Konfigurationspaket als `.zip` Datei verfügbar ist. Wenn Sie das AWS CodeCommit Repository verwenden, achten Sie darauf, das Konfigurationspaket im Repository zu platzieren, ohne die Dateien zu komprimieren. Hinweise zum Erstellen und Speichern des Konfigurationspakets in finden Sie AWS CodeCommit unterLeitfaden zur cFCT-Anpassung.

Sie können das Beispielkonfigurationspaket verwenden, um Ihre eigene benutzerdefinierte Konfigurationsquelle zu erstellen. Wenn Sie bereit sind, Ihre benutzerdefinierten Konfigurationen bereitzustellen, laden Sie das Konfigurationspaket manuell hoch, entweder in den Amazon S3 S3-Bucket oder in das AWS CodeCommit Repository. Die Pipeline beginnt automatisch, wenn Sie die Konfigurationsdatei hochladen.

Wählen Sie Ihre Genehmigungsparameter für die Pipeline-Konfiguration

Die AWS CloudFormation Vorlage bietet die Möglichkeit, die Bereitstellung von Konfigurationsänderungen manuell zu genehmigen. Standardmäßig ist die manuelle Genehmigung nicht aktiviert. Weitere Informationen finden Sie in Schritt 1. Starten Sie den Stack.

Wenn die manuelle Genehmigung aktiviert ist, validiert die Konfigurationspipeline die Anpassungen, die am AWS Control Tower Tower-Dateimanifest und an den Vorlagen vorgenommen wurden, und unterbricht dann den Vorgang, bis die manuelle Genehmigung erteilt wird. Nach der Genehmigung werden bei der Bereitstellung nach Bedarf die verbleibenden Pipeline-Phasen ausgeführt, um die Customizations for AWS Control Tower (cFCT) -Funktionalität zu implementieren.

Sie können den manuellen Genehmigungsparameter verwenden, um zu verhindern, dass die Anpassungen für die AWS Control Tower Tower-Konfiguration ausgeführt werden, indem Sie den ersten Versuch, die Pipeline zu durchlaufen, ablehnen. Dieser Parameter ermöglicht es Ihnen auch, Anpassungen für die AWS Control Tower Tower-Konfigurationsänderungen manuell zu validieren, als letzte Kontrolle vor der Implementierung.

Um Anpassungen für AWS Control Tower zu aktualisieren

Wenn Sie CfCT bereits bereitgestellt haben, müssen Sie den CloudFormation Stack aktualisieren, um die neueste Version des CfCT-Frameworks zu erhalten. Einzelheiten finden Sie unter Update the Stack.

Vorlage und Quellcode

Anpassungen für AWS Control Tower (cFCT) werden in Ihrem Verwaltungskonto bereitgestellt, nachdem Sie Ihre Vorlage gestartet haben. AWS CloudFormation Sie können die Vorlage von herunterladen GitHub und dann von aus starten. AWS CloudFormation

Das customizations-for-aws-control-tower.template stellt Folgendes bereit:

- AWS CodeBuild Ein Projekt
- Ein AWS CodePipeline Projekt

- Eine EventBridge Amazon-Regel
- AWS Lambda Funktionen
- Eine Amazon Simple Queue Service-Warteschlange
- Ein Amazon Simple Storage Service-Bucket mit einem Beispielkonfigurationspaket
- AWS Step Functions

> **Note**
>
> Sie können die Vorlage an Ihre spezifischen Anforderungen anpassen.

Quellcode-Repository

Sie können unser GitHubRepository besuchen, um die Vorlagen und Skripte für CfCT herunterzuladen und Ihre landing zone Zone-Anpassungen mit anderen zu teilen.

Automatisierte Bereitstellung

Bevor Sie die automatisierte Bereitstellung starten, sollten Sie sich die Überlegungen ansehen. Folgen Sie den step-by-step Anweisungen in diesem Abschnitt, um die Lösung in Ihrem AWS Control Tower Tower-Managementkonto zu konfigurieren und bereitzustellen.

Zeit für die Bereitstellung: Ungefähr 15 Minuten

Voraussetzungen

CfCT muss in Ihrem AWS Control Tower Tower-Managementkonto und in Ihrer AWS Control Tower Tower-Heimatregion bereitgestellt werden. Wenn Sie keine landing zone eingerichtet haben, finden Sie weitere Informationen unterErste Schritte.

Schritte zur Bereitstellung

Das Verfahren zur Bereitstellung von CfCT besteht aus zwei Hauptschritten. Ausführliche Anweisungen können über die Links zu den einzelnen Schritten abgerufen werden.

Schritt 1. Starten des -Stacks

- Starten Sie die CloudFormation Vorlage in Ihrem Verwaltungskonto.

- Überprüfen Sie die Vorlagenparameter und passen Sie sie gegebenenfalls an.

Schritt 2. Erstellen Sie ein benutzerdefiniertes Paket

- Erstellen Sie ein benutzerdefiniertes Konfigurationspaket.

> **Important**
>
> Um die richtige AWS CloudFormation Vorlage herunterzuladen und CfCT zu starten, folgen Sie dem GitHub Link in diesem Abschnitt. Folgen Sie keinen älteren Links zu zuvor angegebenen S3-Buckets.

Schritt 1. Starten des -Stacks

Die CloudFormation Vorlage in diesem Abschnitt stellt Anpassungen für AWS Control Tower (cFCT) in Ihrem Konto bereit.

> **Hinweis**
>
> Sie sind für die Kosten der AWS Services verantwortlich, die Sie bei der Ausführung von CfCT in Anspruch nehmen. Weitere Details finden Sie unter Cost (Kosten).

1. Um Anpassungen für AWS Control Tower zu starten, laden Sie die Vorlage von herunter GitHub und starten Sie sie dann von AWS CloudFormation.
2. Die Vorlage wird standardmäßig in der Region USA Ost (Nord-Virginia) gestartet. Um CfCT in einer anderen AWS Region zu starten, verwenden Sie die Regionsauswahl in der Navigationsleiste der Konsole.

   > **Note**
   >
   > cFCT muss in derselben Region und demselben Konto gestartet werden, in der Sie Ihre AWS Control Tower Tower-Landezone bereitgestellt haben, was Ihre Heimatregion ist.

3. Stellen Sie auf der Seite „Stack erstellen“ sicher, dass die richtige Vorlagen-URL im URL-Textfeld angezeigt wird, und wählen Sie Weiter aus.

4. Weisen Sie Ihrem CfCt-Stack auf der Seite „Stack-Details angeben“ einen Namen zu.
5. Überprüfen Sie unter Parameter die folgenden Parameter und ändern Sie sie gegebenenfalls in der Vorlage.

Konfiguration der Pipeline		
Parameter	Standard	Beschreibung
Phase der Genehmigung der Pipeline	`No`	Wählen Sie aus, ob die Pipeline-Konfiguration von der standardmäßigen automatisierten Genehmigungsphase in eine manuelle Genehmigungsphase geändert werden soll. Weitere Informationen finden Sie unter the section called “Leitfaden zur cFCT-Anpassung”.
E-Mail-Adresse für die Pipeline-Genehmigung	<Optional Input>	Die E-Mail-Adresse für Genehmigungsbenachrichtigungen. Um diesen Parameter verwenden zu können, müssen Sie den Parameter Pipeline Approval Stage auf festlegen`Yes`.
CodePipelineAWS-Quelle	`Amazon S3`	Die Quelle für AWS CodePipeline , die Ihnen bei der Auswahl des Speicherorts und der Konfiguration der CfCT-Anpassungen hilft.

CodeCommit AWS-Einrichtung		
Parameter	Standard	Beschreibung
Bestehendes CodeCommit Repository?	`No`	Wählen Sie aus, ob Sie ein vorhandenes CodeCommi t Git-Repository verwenden möchten. Wenn Sie möchten`Yes`, müssen Sie den CodePipeline Source-Parameter auf setzen`AWS CodeCommit` .
CodeCommit Repository-Name	`custom-control-tow er-configuration`	Wenn Sie den Namen eines vorhandenen Git-Repositorys angeben, müssen Sie das Existierende CodeCommit Repository festlegen? Geben Sie den Parameter ein `Yes` und geben Sie den genauen Namen dieses Repositorys ein.
CodeCommit Name der Filiale	`main`	Der Git-Zweig, in dem das Anpassungspaket gespeiche rt ist. Um diesen Parameter zu verwenden, müssen Sie den CodePipeline Source-Parameter auf setzen`AWS CodeCommit` .

CloudFormation StackSets Konfiguration		
Parameter	Standard	Beschreibung
Parallelitätstyp der Region	`PARALLEL`	Wählen Sie den Parallelitätstyp für die Bereitstellung von StackSets Vorgängen in Regionen aus. Diese Einstellung gilt für Workflows zum Erstellen, Aktualisieren und Löschen. Ein anderer zulässiger Wert ist`SEQUENTIAL` .
Maximaler Prozentsatz an gleichzeitigen Vorgängen	`100`	Der maximale Prozentsatz der Konten, auf denen dieser Vorgang gleichzeitig ausgeführt werden kann. Der zulässige Höchstwert ist 100. Weitere Informationen finden Sie unter Stack Set-Betriebsoptionen.
Prozentsatz der Fehlertoleranz	`10`	Der Prozentsatz der Konten pro Region, für die dieser Stack-Vorgang fehlschlagen kann, bevor AWS den Vorgang in dieser Region CloudFormation stoppt. Der zulässige Mindestwert ist 0 und der zulässige Höchstwert ist 100. Weitere Informationen finden Sie unter Stack Set-Betriebsoptionen.

6. Wählen Sie Weiter aus.
7. Wählen Sie auf der Seite Configure stack options (Stack-Optionen konfigurieren) Next (Weiter) aus.

8. Überprüfen und bestätigen Sie die Einstellungen auf der Seite Review. Aktivieren Sie unbedingt das Kontrollkästchen, das bestätigt, dass die Vorlage AWS Identity and Access Management (IAM) erstellt.
9. Wählen Sie Stack erstellen aus, um den Stack bereitzustellen.

   Sie können den Status des Stacks in der CloudFormation Konsole in der Spalte Status einsehen. In etwa 15 Minuten sollte der Status CREATE_COMPLETE angezeigt werden.

Schritt 2. Erstellen Sie ein benutzerdefiniertes Paket

Mit dem gestarteten Stack können Sie Anpassungen zu Ihrer AWS Control Tower Tower-Landing landing zone und Ihren Service Control-Richtlinien (SCPs) hinzufügen, indem Sie das mitgelieferte Konfigurationspaket anpassen. Detaillierte Anweisungen zur Erstellung eines benutzerdefinierten Pakets finden Sie in der. Leitfaden zur cFCT-Anpassung

> **Hinweis**
>
> Die Pipeline kann nicht ausgeführt werden, ohne das benutzerdefinierte Konfigurationspaket hochzuladen.

Aktualisieren Sie den Stack

Wenn Sie bereits Anpassungen für AWS Control Tower (cFCT) bereitgestellt haben, gehen Sie wie folgt vor, um den AWS CloudFormation Stack für die neueste Version des CfCT-Frameworks zu aktualisieren.

> **Important**
>
> Bevor Sie das folgende Verfahren abschließen können, müssen Sie die neueste Vorlage aus GitHub einem Amazon Simple Storage Service (Amazon S3) -Bucket hochladen. Anweisungen zu den ersten Schritten mit Amazon S3 finden Sie unter Erste Schritte mit Amazon S3 im Amazon Simple Storage Service-Benutzerhandbuch.

1. Melden Sie sich an der AWS CloudFormation -Konsole an.
2. Wählen Sie Ihren vorhandenen Customizations for AWS Control Tower (cFCT) CloudFormation -Stack aus und wählen Sie dann Aktualisieren aus.

3. Wählen Sie unter Voraussetzung — Vorlage vorbereiten die Option Aktuelle Vorlage ersetzen aus.
4. Gehen Sie unter Vorlage angeben wie folgt vor:

   a. Wählen Sie als Vorlagenquelle die Option Aktuelle Vorlage ersetzen aus.

   b. Geben Sie für Amazon S3-URL die Vorlagen-URL für die Vorlage ein, von der Sie zuvor GitHub auf Amazon S3 hochgeladen haben, und wählen Sie dann Weiter.

   c. Stellen Sie sicher, dass die Vorlagen-URL korrekt ist. Wählen Sie dann Weiter und erneut Weiter.
5. Überprüfen Sie unter Parameter die Parameter für die Vorlage und ändern Sie sie nach Bedarf. Weitere Informationen finden Sie in Schritt 1. Starten Sie den Stack, um weitere Informationen zu den Parametern zu erhalten.
6. Wählen Sie Weiter aus.
7. Wählen Sie auf der Seite Configure stack options (Stack-Optionen konfigurieren) Next (Weiter) aus.
8. Überprüfen und bestätigen Sie die Einstellungen auf der Seite Review. Achten Sie darauf, das Kästchen anzukreuzen, das bestätigt, dass die Vorlage möglicherweise AWS Identity and Access Management (IAM-) Ressourcen erstellt.
9. Wählen Sie Änderungssatz anzeigen und überprüfen Sie die Änderungen.
10. Wählen Sie Stack aktualisieren, um den Stack bereitzustellen.

    Sie können den Status des Stacks in der AWS CloudFormation Konsole in der Spalte Status einsehen. In etwa 15 Minuten sollte der Status UPDATE_COMPLETE angezeigt werden.

Löschen eines Stack-Sets

Sie können ein Stack-Set löschen, wenn Sie das Löschen von Stack-Sets in der Manifestdatei aktiviert haben. Standardmäßig ist der `enable_stack_set_deletion`-Parameter auf `false` festgelegt. In dieser Konfiguration werden keine Maßnahmen ergriffen, um das zugehörige Stack-Set zu löschen, wenn eine Ressource aus der CFCT-Manifestdatei entfernt wird.

Wenn Sie den Wert von `enable_stack_set_deletion` to `true` in der Manifestdatei ändern, löscht CfcT das Stack-Set und alle zugehörigen Ressourcen, wenn Sie eine zugehörige Ressource aus der Manifestdatei entfernen.

Diese Funktion wird in Version 2 der Manifestdatei unterstützt.

> **Important**
>
> Wenn Sie anfänglich den Wert `enable_stack_set_deletion` auf gesetzt habentrue, werden beim nächsten Aufruf von cfcT ALLE Ressourcen, die mit dem Präfix beginnen`CustomControlTower-`, die über das zugehörige Schlüsseltag `Key:AWS_Solutions, Value: CustomControlTowerStackSet` verfügen und die nicht in der Manifestdatei deklariert sind, zum Löschen zwischengespeichert.

Hier ist ein Beispiel dafür, wie dieser Parameter in einer Datei festgelegt wird: `manifest.yaml`

```
version: 2021-03-15
region: us-east-1
enable_stack_set_deletion: true   #New opt-in functionality


resources:
  - name: demo_resource_1
    resource_file: s3://demo_bucket/resource.template
    deployment_targets:
      accounts:
        - 012345678912
    deploy_method: stack_set
    ...
    regions:
    - us-east-1
    - us-west-2

  - name: demo_resource_2
    resource_file: s3://demo_bucket/resource.template
    deployment_targets:
      accounts:
        - 012345678912
    deploy_method: stack_set
    ...
    regions:
    - us-east-1
    - eu-north-1
```

Amazon S3 als Konfigurationsquelle einrichten

Wenn Sie Anpassungen für AWS Control Tower einrichten, speichert es eine erste Konfigurationsdatei, die als `_custom-control-tower-configuration.zip` Datei bezeichnet wird, in einem Amazon Simple Storage Service (Amazon S3) -Bucket mit dem Namen`custom-control-tower-configuration-`*`account-ID`*`-`*`region`*.

> **Hinweis**
>
> Wenn Sie sich dafür entscheiden, diese Datei herunterzuladen und zu ändern, denken Sie daran, die Änderungen zu komprimieren, als neue Datei mit dem Namen `custom-control-tower-configuration.zip` zu speichern und sie dann wieder in denselben Amazon S3 S3-Bucket hochzuladen.
> Der Amazon S3 S3-Bucket ist die Standardquelle der Pipeline. Wenn die Standardeinstellungen vorhanden sind, wird beim Hochladen einer Konfigurations-ZIP-Datei ohne das Unterstrich-Präfix im Dateinamen in den S3-Bucket die Pipeline automatisch initiiert.

Die ZIP-Datei ist durch serverseitige Verschlüsselung (SSE) mit AWS Key Management Service (AWS KMS) und die Ablehnung der Verwendung des KMS-Schlüssels geschützt. Für den Zugriff auf die ZIP-Datei müssen Sie die KMS-Schlüsselrichtlinie aktualisieren, um die Rolle (n) anzugeben, denen Zugriff gewährt werden soll. Bei der Rolle kann es sich um eine Administratorrolle, einen Benutzer oder beides handeln. Gehen Sie wie folgt vor:

1. Navigieren Sie zur AWS Key Management Service -Konsole.
2. Wählen Sie unter Vom Kunden verwaltete Schlüssel die Option aus CustomControlTowerKMSKey.
3. Wählen Sie die Registerkarte Schlüsselrichtlinie aus. Wählen Sie dann Bearbeiten aus.
4. Suchen Sie auf der Seite „Schlüsselrichtlinie bearbeiten“ im Code nach dem Abschnitt „Verwendung des Schlüssels zulassen“ und fügen Sie eine der folgenden Berechtigungen hinzu:
   - So fügen Sie eine Administratorrolle hinzu:

     `arn:aws:iam::`*`<account-ID>`*`:role/`*`<administrator-role>`*
   - Um einen Benutzer hinzuzufügen:

     `arn:aws:iam::`*`<account-ID>`*`:user/`*`<username>`*
5. Wählen Sie Save Changes (Änderungen speichern).

6. Navigieren Sie zur Amazon S3 S3-Konsole, suchen Sie den S3-Bucket, der die Konfigurations-ZIP-Datei enthält, und wählen Sie Herunterladen aus.
7. Nehmen Sie die erforderlichen Konfigurationsänderungen an der Manifestdatei und den Vorlagendateien vor. Informationen zum Anpassen der Manifest- und Vorlagendateien finden Sie unterthe section called “Leitfaden zur cFCT-Anpassung”.
8. Laden Sie Ihre Änderungen hoch:
   a. Komprimieren Sie die geänderten Konfigurationsdateien und geben Sie der Datei einen Namen:`custom-control-tower-configuration.zip`.
   b. Laden Sie die Datei mithilfe von SSE mit dem AWS KMS Master-Key auf Amazon S3 hoch:. `CustomControlTowerKMSKey`

GitHub Als Konfigurationsquelle einrichten

In diesem Abschnitt erfahren Sie, wie Sie Anpassungen für AWS Control Tower (cFCT) GitHub als Quelle bereitstellen. Der Prozess besteht aus drei Hauptschritten:

- Bereite ein GitHub Repository vor
- Erstellen Sie die GitHub Codeverbindung
- Stellen Sie den CloudFormation Stack bereit

Bereite ein GitHub Repository vor

Erstellen Sie ein Repository in Ihrem GitHub Konto. Der Standardname, der in der Vorlage verwendet wird, lautet`custom-control-tower-configuration`. Erwägen Sie, das Ziel-Repository als privat zu kennzeichnen. Sie definieren Ihre Anpassungen in einer `yaml` Datei mit dem Namen `manifest.yaml` im Deployment-Ordner des cFCT-Repositorys.

Das cFCT-Anpassungsleitfaden enthält eine detaillierte Anleitung zur Erstellung und Konfiguration `manifest.yaml` Ihrer Anpassungen.

Erstellen Sie die Verbindung GitHub

Führen Sie in Ihrer Developer Tools --Connections-Instanz für Github die folgenden Schritte aus:

1. Wählen Sie Verbindung erstellen und wählen Sie GitHub als Anbieter

2. Wählen Sie GitHub App-Verbindung erstellen und geben Sie im Feld Verbindungsname GitHub cFCT oder einen beliebigen Namen ein
3. Wählen Sie Verbinden mit aus GitHub und wählen Sie dann Neue App installieren
4. Wähle den GitHub Benutzer oder die Organisation für dein Repository
5. Wählen Sie unter Repository-Zugriff die Option Nur Repositorys auswählen aus, wählen Sie dann das zuvor erstellte Repository aus und speichern Sie Ihre Arbeit.
6. Notieren Sie sich den Code Connections-ARN — Sie benötigen ihn, wenn Sie den CloudFormation Stack bereitstellen.

Stellen Sie das bereit CloudFormation Stack

- Laden Sie die `custom-control-tower-initiation.template` Datei aus dem Repository herunter.
- Erstellen Sie mithilfe der `custom-control-tower-initiation.template` Datei einen neuen CloudFormation Stapel.
- Wählen Sie unter AWS CodePipeline Quelle die Option GitHub (über Codeverbindung).
- Geben Sie unter GitHub Setup die folgenden Felder an:
  - Geben Sie für den ARN der Codeverbindung den ARN der Codeverbindung an
  - Geben Sie für GitHub Benutzer oder Organisation den Namen des GitHub Benutzers oder der Organisation an, unter dem Sie das Repository erstellt haben
  - Geben Sie für GitHub Repository-Name den Repository-Namen ein (standardmäßig) `custom-control-tower-configuration`
  - Geben Sie für GitHub Branch Name den Branch-Namen ein (standardmäßig) `main`

Erfassung von Betriebskennzahlen

Anpassungen für AWS Control Tower (cFCT) beinhalten eine Option zum Senden anonymer Betriebsmetriken an. AWS AWS verwendet diese Daten, um zu verstehen, wie Kunden CfCT sowie andere verwandte Dienstleistungen und Produkte nutzen. Wenn die Datenerfassung aktiviert ist, werden die folgenden Informationen gesendet an AWS:

- Lösungs-ID: Die AWS Lösungs-ID
- Eindeutige ID (UUID): Zufällig generierte, eindeutige Kennung für jede Bereitstellung

- Zeitstempel: Zeitstempel der Datenerfassung
- Anzahl der ausgeführten Zustandsmaschinen: Zählt inkrementell, wie oft diese Zustandsmaschine ausgeführt wird
- Manifestversion: Die in der Konfiguration verwendete Manifestversion

> **Note**
>
> AWS besitzt die gesammelten Daten. Die Datenerfassung unterliegt der AWS Datenschutzrichtlinie.

Um das Senden anonymer Betriebsdaten an zu deaktivieren AWS, führen Sie eine der folgenden Aufgaben aus:

- Aktualisieren Sie den Abschnitt zur AWS CloudFormation Vorlagenzuweisung wie folgt:

  von

  ```
  AnonymousData:
       SendAnonymousData:
          Data: Yes
  ```

  auf

  ```
  AnonymousData:
       SendAnonymousData:
          Data: No
  ```

- Suchen Sie nach der Bereitstellung von CfCT den **`/org/primary/metrics_flag`** SSM-Parameterschlüssel in der Parameter Store-Konsole und aktualisieren Sie den Wert auf. **`No`**

Leitfaden zur cFCT-Anpassung

Der Leitfaden Anpassungen für den AWS Control Tower (cFCT) richtet sich an Administratoren, DevOps Fachleute, unabhängige Softwareanbieter, IT-Infrastrukturarchitekten und Systemintegratoren, die ihre AWS Control Tower-Umgebungen an ihr Unternehmen und ihre Kunden

anpassen und erweitern möchten. Es enthält Informationen zur Anpassung und Erweiterung der AWS Control Tower-Umgebung mit dem cFCT-Anpassungspaket.

> **Note**
>
> Für die Bereitstellung und Konfiguration (cFCT) müssen Sie ein Konfigurationspaket bereitstellen und verarbeiten. AWS CodePipeline In den folgenden Abschnitten wird der Vorgang ausführlich beschrieben.

Überblick über die Code-Pipeline

Das Konfigurationspaket erfordert Amazon Simple Storage Service (Amazon S3) und AWS CodePipeline. Das Konfigurationspaket enthält die folgenden Elemente:

- Eine Manifestdatei
- Ein dazugehöriger Satz von Vorlagen
- Andere JSON-Dateien zur Beschreibung und Implementierung Ihrer Anpassungen an Ihre AWS Control Tower-Umgebung

Standardmäßig wird das `_custom-control-tower-configuration.zip` Konfigurationspaket in einen Amazon S3-Bucket mit der folgenden Namenskonvention geladen:

`custom-control-tower-configuration-`*`accountID`*`-`*`region`*.

> **Note**
>
> Standardmäßig erstellt cFCT einen Amazon S3-Bucket zum Speichern der Pipeline-Quelle. Die meisten Kunden bleiben bei dieser Standardeinstellung. Wenn Sie ein vorhandenes AWS CodeCommit Repository haben, können Sie den Quellspeicherort in Ihr AWS CodeCommit Repository ändern. Weitere Informationen finden Sie CodePipeline im AWS CodePipeline Benutzerhandbuch unter Bearbeiten einer Pipeline.

Die Manifestdatei ist eine Textdatei, die die AWS Ressourcen beschreibt, die Sie zur Anpassung Ihrer Landezone einsetzen können. CodePipeline erledigt diese Aufgaben:

- extrahiert die Manifestdatei, den dazugehörigen Vorlagensatz und andere JSON-Dateien

- führt Manifest- und Vorlagenvalidierungen durch
- ruft Abschnitte in der cFCT-Manifestdatei auf, um bestimmte Pipeline-Phasen auszuführen. ???

Wenn Sie das Konfigurationspaket aktualisieren, indem Sie die Manifestdatei anpassen und den Unterstrich (_) aus dem Dateinamen des Konfigurationspakets entfernen, wird es automatisch initiiert. AWS CodePipeline

> **Merken Sie sich den Unterstrich**
>
> Der Dateiname des Beispielkonfigurationspakets beginnt mit einem Unterstrich (_), sodass dieser nicht automatisch AWS CodePipeline ausgelöst wird. Wenn Sie die Anpassung des Konfigurationspakets abgeschlossen haben, laden Sie die Datei `custom-control-tower-configuration.zip` ohne Unterstrich (_) hoch, um die Bereitstellung auszulösen. AWS CodePipeline

AWS CodePipeline Stufen

Die cFCT-Pipeline erfordert mehrere AWS CodePipeline Phasen, um Ihre AWS Control Tower-Umgebung zu implementieren und zu aktualisieren.

1. Quellphase

   Die Quellphase ist die Anfangsphase. Ihr benutzerdefiniertes Konfigurationspaket initiiert diese Pipeline-Phase. Die Quelle für den AWS CodePipeline kann entweder ein Amazon S3-Bucket oder ein AWS CodeCommit Repository sein, in dem das Konfigurationspaket gehostet werden kann.

2. Phase erstellen

   In der Build-Phase AWS CodeBuild muss der Inhalt des Konfigurationspakets überprüft werden. Zu diesen Prüfungen gehört das Testen der `manifest.yaml` Dateisyntax und des Schemas sowie aller im Paket enthaltenen oder remote gehosteten CloudFormation Vorlagen mithilfe von CloudFormation `validate-template` und`cfn_nag`. Wenn die Manifestdatei und die CloudFormation Vorlagen die Tests bestehen, fährt die Pipeline mit der nächsten Phase fort. Wenn die Tests fehlschlagen, können Sie die CodeBuild Protokolle überprüfen, um das Problem zu identifizieren, und die Konfigurationsquelldatei nach Bedarf bearbeiten.

3. Phase der manuellen Genehmigung (optional)

Die manuelle Genehmigungsphase ist optional. Wenn Sie diese Phase aktivieren, bietet sie zusätzliche Kontrolle über die Konfigurationspipeline. Die Pipeline wird während der Bereitstellung angehalten, bis eine Genehmigung erteilt wird. Sie können sich für die manuelle Genehmigung entscheiden, indem Sie den Parameter Pipeline-Genehmigungsphase auf Ja ändern, wenn Sie den Stack starten.

4. Phase „Service Control Policy“

   In der Phase Service Control Policy wird die Service Control Policy (SCP) -Zustandsmaschine aufgerufen, um AWS Organizations APIs aufzurufen, die SCPs erstellen.

5. Phase „Resource Control Policy“

   Der Resource Control Policy-Schritt ruft die RCP-Zustandsmaschine (Resource Control Policy) auf, um AWS Organizations APIs aufzurufen, die RCPs erstellen.

6. CloudFormation Ressourcenphase

   Die CloudFormation Ressourcenphase ruft den Stack Set State Machine auf, um die Ressourcen bereitzustellen, die in der Liste der Konten oder Organisationseinheiten (OUs) angegeben sind, die Sie in der Manifestdatei angegeben haben. Die State Machine erstellt die CloudFormation Ressourcen in der Reihenfolge, in der sie in der Manifestdatei angegeben sind. Um eine Ressourcenabhängigkeit anzugeben, ordnen Sie die Reihenfolge an, in der Ressourcen in der Manifestdatei angegeben werden. Die Reihenfolge der Ressourcen in der Manifestdatei ist die einzige Möglichkeit, eine Abhängigkeit anzugeben.

Definieren Sie eine benutzerdefinierte Konfiguration

Sie definieren Ihre benutzerdefinierte AWS Control Tower-Konfiguration mit der cFCT-Manifestdatei, dem zugehörigen Vorlagensatz und anderen JSON-Dateien. Sie packen diese Dateien in eine Ordnerstruktur und platzieren sie als `.zip` Datei im Amazon S3-Bucket, wie im folgenden Codebeispiel gezeigt.

Benutzerdefinierte Konfigurationsordnerstruktur

```
- manifest.yaml
- policies/                                                [optional]
   - service control policies files (*.json)
- templates/                                               [optional]
   - template files for AWS CloudFormation Resources (*.template)
```

Das vorherige Beispiel zeigt die Struktur eines benutzerdefinierten Konfigurationsordners. Die Ordnerstruktur bleibt gleich, unabhängig davon, ob Sie Amazon S3 oder ein AWS CodeCommit Repository als Quellspeicherort wählen. Wenn Sie Amazon S3 als Quellspeicher wählen, komprimieren Sie alle Ordner und Dateien in einer `custom-control-tower-configuration.zip` Datei und laden Sie nur die `.zip` Datei in den angegebenen Amazon S3-Bucket hoch.

> **Note**
>
> Wenn Sie es verwenden AWS CodeCommit, platzieren Sie die Dateien im Repository, ohne die Dateien zu komprimieren.

Die cFCT-Manifestdatei

Die `manifest.yaml` cFCT-Datei ist eine Textdatei, die Ihre AWS Ressourcen beschreibt. Das folgende Beispiel zeigt die Struktur der cFCT-Manifestdatei.

```
---
region: String
version: 2021-03-15

resources:
  #set of CloudFormation resources, SCP policies, or RCP policies
...
```

Wie im vorherigen Codebeispiel gezeigt, geben die ersten beiden Zeilen der Manifestdatei die Werte der Schlüsselwörter Region und Version an. Hier sind die Definitionen dieser Schlüsselwörter.

region — Eine Textzeichenfolge für die Standardregion des AWS Control Tower. Dieser Wert muss ein gültiger AWS Regionsname sein (z. B. `us-east-1`eu-west-1, oderap-southeast-1). Die AWS-Control-Tower-Heimatregion ist die Standardeinstellung, wenn Sie benutzerdefinierte AWS Control Tower-Ressourcen (z. B. CloudFormation StackSets) erstellen, sofern keine ressourcenspezifischere Region angegeben ist.

```
region:your-home-region
```

Version — Die Versionsnummer des Manifestschemas. Die neueste unterstützte Version ist 2021-03-15.

```
version: 2021-03-15
```

> **Note**
>
> Wir empfehlen dringend, die neueste Version zu verwenden. Informationen zum Aktualisieren der Manifesteigenschaften in der neuesten Version finden Sie unterVersions-Upgrades für das cFCT-Manifest.

Das nächste Schlüsselwort, das im vorherigen Beispiel gezeigt wurde, ist das Schlüsselwort resources. Der Ressourcenbereich der Manifestdatei ist stark strukturiert. Er enthält eine detaillierte Liste von AWS Ressourcen, die automatisch von der cFCT-Pipeline bereitgestellt werden. Diese Beschreibungen der Ressourcen und ihrer verfügbaren Parameter finden Sie im nächsten Abschnitt.

Der Abschnitt „Ressourcen“ der cFCT-Manifestdatei

In diesem Thema wird der Abschnitt Ressourcen der cFCT-Manifestdatei beschrieben, in dem Sie die Ressourcen definieren, die für Ihre Anpassungen erforderlich sind. Dieser Abschnitt der cFCT-Manifestdatei beginnt bei den Schlüsselwortressourcen und setzt sich bis zum Ende der Datei fort.

Der Ressourcenabschnitt der Manifestdatei spezifiziert die CloudFormation StackSets AWS Organizations SCPs und RCPs, die CfCT automatisch über die Codepipeline bereitstellt. Sie können OUs, Konten und Regionen für die Bereitstellung von Stack-Instances auflisten.

Stack-Instances werden auf Kontoebene statt auf OU-Ebene bereitgestellt. SCPs und RCPs werden auf OU-Ebene bereitgestellt. Weitere Informationen finden Sie unter Erstellen Sie Ihre eigenen Anpassungen.

Die folgende Beispielvorlage beschreibt die möglichen Einträge, die für den Ressourcenabschnitt der Manifestdatei verfügbar sind.

```
resources: # List of resources
  - name: [String]
    resource_file: [String] [Local File Path, S3 URI, S3 URL]
    deployment_targets: # account and/or organizational unit names
      accounts: # array of strings, [0-9]{12}
        - 012345678912
        - AccountName1
      organizational_units: #array of strings
        - OuName1
```

```
      - OuName2
  deploy_method: scp | stack_set | rcp
  parameters: # List of parameters [SSM, Alfred, Values]
    - parameter_key: [String]
      parameter_value: [String]
  export_outputs: # list of ssm parameters to store output values
    - name: /org/member/test-ssm/app-id
      value: $[output_ApplicationId]
  regions: #list of strings
  - [String]
```

Der Rest dieses Themas enthält detaillierte Definitionen für die im vorherigen Codebeispiel gezeigten Schlüsselwörter.

name — Der Name, der mit dem verknüpft ist CloudFormation StackSets.
Die von Ihnen angegebene Zeichenfolge weist einem Stack-Set einen benutzerfreundlicheren Namen zu.

- Typ: Zeichenfolge
- Erforderlich: Ja
- Gültige Werte: a-z A-Z, 0-9 und ein Bindestrich (-). Der Name muss mit einem alphabetischen Zeichen beginnen.

Beschreibung — Die Beschreibung der Ressource.

- Typ: Zeichenfolge
- Required: No

resource_file — Diese Datei kann als relativer Speicherort zur Manifestdatei angegeben werden. Dabei handelt es sich um eine Amazon S3-URI oder URL, die auf eine CloudFormation Vorlage oder eine AWS Organizations Service Control-Richtlinie in JSON zum Erstellen von CloudFormation Ressourcen, SCPs oder RCPs verweist.

- Typ: Zeichenfolge
- Erforderlich: Ja

1. Das folgende Beispiel zeigt die`resource_file`, als relativer Speicherort zur Ressourcendatei im Konfigurationspaket angegeben.

```
resources:
  - name: SecurityRoles
    resource_file: templates/custom-security.template
```

2. Das folgende Beispiel zeigt die als Amazon S3-URI angegebene Ressourcendatei

```
resources:
  - name: SecurityRoles
    resource_file: s3://amzn-s3-demo-bucket/[key-name]
```

3. Das folgende Beispiel zeigt die Ressourcendatei, die als Amazon S3-HTTPS-URL angegeben wurde

```
resources:
  - name: SecurityRoles
    resource_file: https://bucket-name.s3.Region.amazonaws.com/key-name
```

> **Note**
>
> Wenn Sie eine Amazon S3-URL angeben, stellen Sie sicher, dass die Bucket-Richtlinie den Lesezugriff für das AWS Control Tower-Verwaltungskonto zulässt, von dem aus Sie cFCT bereitstellen. Wenn Sie eine Amazon S3-HTTPS-URL angeben, stellen Sie sicher, dass der Pfad die Punktnotation verwendet. Beispiel, `S3.us-west-1`. cFCT unterstützt keine Endpunkte, die einen Bindestrich zwischen S3 und der Region enthalten, wie z. B. `S3-us-west-2`

4. Das folgende Beispiel zeigt eine Amazon S3-Bucket-Richtlinie und einen ARN, in dem Ressourcen gespeichert werden.

```
{
   "Version": "2012-10-17",
   "Statement": [
       {
        "Effect": "Allow",
        "Principal": {"AWS": "arn:aws:iam::AccountId:root"},
        "Action": "s3:GetObject",
        "Resource": "arn:aws:s3:::my-bucket/*”
       }
   ]
```

```
}
```

Sie ersetzen die im Beispiel gezeigte *AccountId* Variable durch die AWS Konto-ID für das Verwaltungskonto, das cFCT bereitstellt. Weitere Beispiele finden Sie unter Beispiele für Bucket-Richtlinien im Amazon Simple Storage Service-Benutzerhandbuch.

Parameter — Gibt den Namen und den Wert für CloudFormation Parameter an.

- Type MapList:
- Required: No

Der Parameterabschnitt enthält key/value Parameterpaare. Die folgende Pseudovorlage beschreibt den Parameterabschnitt.

```
parameters:
  - parameter_key: [String]
    parameter_value: [String]
```

- parameter_key — Der dem Parameter zugeordnete Schlüssel.
  - Typ: Zeichenfolge
  - Erforderlich: Ja (unter der Parameter-Eigenschaft)
  - Gültige Werte: a-z und A-Z 0-9
- parameter_value — Der dem Parameter zugeordnete Eingabewert.
  - Typ: Zeichenfolge
  - Erforderlich: Ja (unter der Parameter-Eigenschaft)

deploy_method — Die Bereitstellungsmethode für die Bereitstellung von Ressourcen im Konto. Derzeit unterstützt deploy_method die Bereitstellung von Ressourcen mithilfe der `stack_set` Option für die Bereitstellung von Ressourcen über CloudFormation StackSets, der `scp` Option, wenn Sie SCPs bereitstellen, oder der `rcp` Option, wenn Sie RCPs bereitstellen.

- Typ: Zeichenfolge
- Zulässige Werte: `stack_set` | `scp` | `rcp`
- Erforderlich: Ja

deployment_targets — Liste der Konten oder Organisationseinheiten (OUs), in denen CfCT die Ressourcen bereitstellt, angegeben als accounts oder organizational_units. CloudFormation

> **Note**
>
> Wenn Sie ein SCP oder RCP bereitstellen möchten, muss das Ziel eine OU sein, kein Konto.

- Geben Sie Folgendes ein: Zeichenkettenliste `account name` oder `account number` um anzugeben, dass diese Ressource in der angegebenen Kontenliste bereitgestellt wird, oder 0U `names` um anzugeben, dass diese Ressource in der angegebenen OU-Liste bereitgestellt wird.
- Erforderlich: Mindestens eines der Konten oder Organisationseinheiten
  - Konten:

    Typ: Zeichenkettenliste `account name` oder `account number` um anzugeben, dass diese Ressource in die angegebene Kontenliste aufgenommen wird.
  - organisationale Einheiten:

    Typ: Eine Liste mit einer Zeichenfolge0U `names`, die angibt, dass diese Ressource in einer bestimmten OU-Liste bereitgestellt wird. Wenn Sie eine Organisationseinheit angeben, die keine Konten enthält und die Accounts-Eigenschaft nicht hinzugefügt wird, erstellt cFCT nur das Stack-Set.

    > **Note**
    >
    > Die Verwaltungskonto-ID der Organisation ist kein zulässiger Wert. cFCT unterstützt standardmäßig nicht die Bereitstellung von Stack-Instances im Verwaltungskonto der Organisation. Wenn Sie einen speziellen Anwendungsfall haben, finden Sie weitere Informationen unter Root OU.

export_outputs — Liste von name/value Paaren, die SSM-Parameterschlüssel bezeichnen. Mit diesen SSM-Parameterschlüsseln können Sie Vorlagenausgaben im SSM-Parameterspeicher speichern. Die Ausgabe ist als Referenz für andere Ressourcen vorgesehen, die zuvor in der Manifestdatei definiert wurden.

```
export_outputs: # List of SSM parameters
  - name: [String]
```

```
    value: [String]
```

- Typ: Liste der Schlüsselpaare für Name und Wert. Der Name enthält die `name` Zeichenfolge eines SSM-Parameterspeicherschlüssels, und der Wert enthält die `value` Zeichenfolge des Parameters.
- Gültige Werte: Jede Zeichenfolge oder die `$[output_`*`CfnOutput-Logical-ID`*`]` Variable, die der Vorlagen-Ausgabevariablen *`CfnOutput-Logical-ID`* entspricht. Weitere Informationen zum Abschnitt Ausgaben in einer CloudFormation Vorlage finden Sie im CloudFormation Benutzerhandbuch unter Ausgaben.
- Required: No

Im folgenden Codeausschnitt wird beispielsweise die `VPCID` Vorlagenausgabevariable im benannten SSM-Parameterschlüssel gespeichert. `/org/member/audit/vpc_id`

```
export_outputs: # List of SSM parameters
  - name: /org/member/audit/VPC-ID
    value: $[output_VPCID]
```

> **Note**
>
> Der Schlüsselname export_outputs kann einen anderen Wert als enthalten. `output` Wenn der Name beispielsweise lautet`/org/environment-name`, kann der Wert lauten. `production`

regions — Liste der Regionen, in denen cFCT die CloudFormation Stack-Instances bereitstellt.

- Typ: Eine beliebige Liste AWS kommerzieller Regionsnamen, um anzugeben, dass diese Ressource in der angegebenen Regionsliste eingesetzt wird. Wenn dieses Schlüsselwort in der Manifestdatei nicht vorhanden ist, werden die Ressourcen nur in der Heimatregion bereitgestellt.
- Required: No

Root-OU

cFCT unterstützt Root als Wert für eine Organisationseinheit (OU) `organizational_units` in der Manifest V2-Version (2021-03-15).

- Wenn Sie die Bereitstellungsmethode von `scp` oder`rcp`, wenn Sie Root unter hinzufügen`organizational_units`, wendet AWS Control Tower die Richtlinien auf alle Organisationseinheiten unter Root an. Wenn Sie die Bereitstellungsmethode wählen und Root unter hinzufügen`organizational_units`, stellt cFCT die Stack-Sets in allen Konten unter dem Root bereit, die im AWS Control Tower registriert sind, mit Ausnahme des Verwaltungskontos. `stack_set`
- Gemäß den bewährten Methoden von AWS Control Tower ist das Verwaltungskonto nur für die Verwaltung von Mitgliedskonten und für Abrechnungszwecke vorgesehen. Führen Sie keine Produktions-Workloads im AWS Control Tower-Verwaltungskonto aus.

  Gemäß den Richtlinien für bewährte Methoden untersteht das Verwaltungskonto bei der Bereitstellung von AWS Control Tower der Root-Organisationseinheit, sodass es vollen Zugriff hat und keine zusätzlichen Ressourcen verwendet werden. Aus diesem Grund wird die AWSControlTowerExecution Rolle dem Verwaltungskonto nicht zugewiesen.
- Wir empfehlen, dass Sie diese bewährten Methoden für das Verwaltungskonto befolgen. Wenn Sie einen bestimmten Anwendungsfall haben, der die Bereitstellung von Stacksets im Verwaltungskonto erfordert, schließen Sie Konten als Bereitstellungsziel ein und geben Sie das Verwaltungskonto an. Andernfalls sollten Sie Konten nicht als Bereitstellungsziel angeben. Sie müssen die fehlenden Ressourcen, einschließlich der erforderlichen IAM-Rollen, im Verwaltungskonto erstellen.

Um Stacksets im Verwaltungskonto bereitzustellen, geben Sie es `accounts` als Bereitstellungsziel an und geben Sie das Verwaltungskonto an. Schließen Sie andernfalls keine Konten als Bereitstellungsziel ein.

```
---
region: your-home-region
version: 2021-03-15

resources:

  …truncated…

    deployment_targets:
      organizational_units:
        - Root
```

> **Note**
>
> Die Root-OU-Funktion wird nur in der V2-Version der Manifestdatei (15.03.2021) unterstützt. Wenn Sie Root als OU unter hinzufügen`organizational_units`, fügen Sie keine anderen Organisationseinheiten hinzu.

Verschachtelte Organisationseinheit

cFCT unterstützt das Auflisten einer oder mehrerer verschachtelter OUs unter dem `organizational_units` Schlüsselwort in der Manifest V2-Version (2021-03-15).

Ein vollständiger Pfad (ohne Root) für die verschachtelte Organisationseinheit ist erforderlich, wobei ein Doppelpunkt als Trennzeichen zwischen den Organisationseinheiten verwendet wird. Bei der Bereitstellungsmethode `scp` oder `rcp` der Methode stellt AWS Control Tower die SCPs oder RCPs für die letzte Organisationseinheit im geschachtelten OU-Pfad bereit. Bei der Bereitstellungsmethode `stack_set` stellt AWS Control Tower die Stack-Sets für alle Konten unter der letzten Organisationseinheit im geschachtelten OU-Pfad bereit.

Betrachten Sie zum Beispiel den Pfad. `OUName1:OUName2:OUName3` Die letzte OU im Pfad ist`OUName3`. CfCT stellt die SCPs oder RCPs nur für alle Konten bereit `OUName3` und stapelt sie nur auf allen Konten, die direkt untergeordnet sind. `OUName3`

```
---
region: your-home-region
version: 2021-03-15

resources:

  …truncated…

    deployment_targets:
      organizational_units:
        - OuName1:OUName2:OUName3
```

> **Note**
>
> Die Funktion für verschachtelte Organisationseinheiten wird nur in der V2-Version der Manifestdatei (15.03.2021) unterstützt.

Erstellen Sie Ihre eigenen Anpassungen

Um Ihre eigenen Anpassungen zu erstellen, können Sie die `manifest.yaml` cFCT-Datei ändern, indem Sie Service Control Policies (SCPs), Resource Control Policies (RCPs) und Ressourcen hinzufügen oder aktualisieren. CloudFormation Für Ressourcen, die bereitgestellt werden müssen, können Sie Konten und Organisationseinheiten hinzufügen oder entfernen. Sie können die Vorlagen in den Paketordnern hinzufügen oder ändern, Ihre eigenen Ordner erstellen und auf die Vorlagen oder Ordner in der `manifest.yaml` Datei verweisen.

In diesem Abschnitt werden die beiden Hauptteile der Erstellung Ihrer eigenen Anpassungen erläutert:

- wie Sie Ihr eigenes Konfigurationspaket für Service Control-Richtlinien einrichten
- wie richte ich mein eigenes Konfigurationspaket für AWS CloudFormation Stack-Sets ein

Richten Sie ein Konfigurationspaket für SCPs oder RCPs ein

In diesem Abschnitt wird erklärt, wie Sie ein Konfigurationspaket für Service Control Policies (SCPs) oder Resource Control Policies (RCPs) erstellen. Die beiden Hauptteile dieses Prozesses sind (1) die Vorbereitung der cFCT-Manifestdatei und (2) die Vorbereitung Ihrer Ordnerstruktur.

Schritt 1: Bearbeiten Sie die Datei manifest.yaml

Verwenden Sie die `manifest.yaml` Beispieldatei als Ausgangspunkt. Geben Sie alle erforderlichen Konfigurationen ein. Fügen Sie die `deployment_targets` Details `resource_file` und hinzu.

Der folgende Ausschnitt zeigt die Standardmanifestdatei.

```
---
region: us-east-1
version: 2021-03-15

resources: []
```

Der Wert für `region` wird während der Bereitstellung automatisch hinzugefügt. Er muss der Region entsprechen, in der Sie cFCT bereitgestellt haben. Diese Region muss mit der AWS Control Tower-Region identisch sein.

Um dem `example-configuration` Ordner in dem im Amazon S3-Bucket gespeicherten Zip-Paket einen benutzerdefinierten SCP oder RCP hinzuzufügen, öffnen Sie die `example-manifest.yaml` Datei und beginnen Sie mit der Bearbeitung.

```
---
region: your-home-region
version: 2021-03-15

resources:
  - name: test-preventive-controls
    description: To prevent from deleting or disabling resources in member accounts
    resource_file: policies/preventive-controls.json
    deploy_method: scp | rcp
    #Apply to the following OU(s)
    deployment_targets:
      organizational_units: #array of strings
        - OUName1
        - OUName2

…truncated…
```

Der folgende Ausschnitt zeigt ein Beispiel für eine benutzerdefinierte Manifestdatei. Sie können mit einer einzigen Änderung mehr als eine Richtlinie hinzufügen.

```
---
region: us-east-1
version: 2021-03-15

resources:
  - name: block-s3-public-access
    description: To S3 buckets to have public access
    resource_file: policies/block-s3-public.json
    deploy_method: scp | rcp
    #Apply to the following OU(s)
    deployment_targets:
      organizational_units: #array of strings
        - OUName1
        - OUName2
```

Schritt 2: Erstellen Sie eine Ordnerstruktur

Sie können diesen Schritt überspringen, wenn Sie eine Amazon S3-URL für die Ressourcendatei verwenden und Parameter mit key/value Paaren verwenden.

Sie müssen eine SCP-Richtlinie oder RCP-Richtlinie im JSON-Format angeben, um das Manifest zu unterstützen, da die Manifestdatei auf die JSON-Datei verweist. Stellen Sie sicher, dass die Dateipfade mit den Pfadinformationen in der Manifestdatei übereinstimmen.

- Eine Richtlinien-JSON-Datei enthält die SCPs oder RCPs, die für OUs bereitgestellt werden sollen.

Der folgende Ausschnitt zeigt die Ordnerstruktur für die Beispiel-Manifestdatei.

```
- manifest.yaml
- policies/
   - block-s3-public.json
```

Der folgende Ausschnitt ist ein Beispiel für eine Richtliniendatei. `block-s3-public.json`

JSON

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"GuardPutAccountPublicAccessBlock",
         "Effect":"Deny",
         "Action":"s3:PutAccountPublicAccessBlock",
         "Resource":"arn:aws:s3:::*"
      }
   ]
}
```

Richten Sie ein Konfigurationspaket ein für CloudFormation StackSets

In diesem Abschnitt wird erklärt, wie Sie ein Konfigurationspaket für CloudFormation StackSets einrichten. Die beiden Hauptteile dieses Prozesses sind: (1) die Manifestdatei vorbereiten und (2) die Ordnerstruktur aktualisieren.

Schritt 1: Bearbeiten Sie die vorhandene Manifestdatei

Fügen Sie die neuen CloudFormation StackSets Informationen zur Manifestdatei hinzu, die Sie zuvor bearbeitet haben.

Nur zur Überprüfung: Der folgende Ausschnitt enthält dieselbe benutzerdefinierte Manifestdatei, die zuvor zum Einrichten eines Konfigurationspakets für SCPs oder RCPs angezeigt wurde. Jetzt können Sie diese Datei weiter bearbeiten, um die Details zu Ihren Ressourcen einzubeziehen.

```
---
region: us-east-1
version: 2021-03-15

resources:

  - name: block-s3-public-access
    description: To S3 buckets to have public access
    resource_file: policies/block-s3-public.json
    deploy_method: scp | rcp
    #Apply to the following OU(s)
    deployment_targets:
    organizational_units: #array of strings
    - OUName1
    - OUName2
```

Der folgende Ausschnitt zeigt eine bearbeitete Beispiel-Manifestdatei, die die Details enthält. `resources` Die Reihenfolge von `resources` bestimmt die Ausführungsreihenfolge für die Erstellung von `resources` Abhängigkeiten. Sie können die folgende Beispiel-Manifestdatei gemäß Ihren Geschäftsanforderungen bearbeiten.

```
---
region: your-home-region
version: 2021-03-15

…truncated…

resources:
  - name: stackset-1
    resource_file: templates/create-ssm-parameter-keys-1.template
    parameters:
      - parameter_key: parameter-1
        parameter_value: value-1
```

```
    deploy_method: stack_set
    deployment_targets:
      accounts: # array of strings, [0-9]{12}
        - account number or account name
        - 123456789123
      organizational_units: #array of strings, ou ids, ou-xxxx
        - OuName1
        - OUName2
    export_outputs:
      - name: /org/member/test-ssm/app-id
        value: $[output_ApplicationId]
    regions:
      - region-name

  - name: stackset-2
    resource_file: s3://bucket-name/key-name
    parameters:
      - parameter_key: parameter-1
        parameter_value: value-1
    deploy_method: stack_set
    deployment_targets:
      accounts: # array of strings, [0-9]{12}
        - account number or account name
        - 123456789123
      organizational_units: #array of strings
        - OuName1
        - OUName2
regions:
  - region-name
```

Das folgende Beispiel zeigt, dass Sie der Manifestdatei mehr als eine CloudFormation Ressource hinzufügen können.

```
---
region: us-east-1
version: 2021-03-15

resources:
  - name: block-s3-public-access
    description: To S3 buckets to have public access
    resource_file: policies/block-s3-public.json
    deploy_method: scp | rcp
    #Apply to the following OU(s)
```

```
    deployment_targets:
      organizational_units: #array of strings
        - Custom
        - Sandbox

  - name: transit-network
    resource_file: templates/transit-gateway.template
    parameter_file: parameters/transit-gateway.json
    deploy_method: stack_set
    deployment_targets:
      accounts: # array of strings, [0-9]{12}
        - Prod
        - 123456789123 #Network
      organizational_units: #array of strings
        - Custom
    export_outputs:
      - name: /org/network/transit-gateway-id
        value: $[output_TransitGatewayID]
    regions:
      - us-east-1
```

Schritt 2: Aktualisieren Sie die Ordnerstruktur

Wenn Sie die Ordnerstruktur aktualisieren, können Sie alle unterstützenden CloudFormation Vorlagendateien und SCP- oder RCP-Richtliniendateien einbeziehen, die sich in der Manifestdatei befinden. Stellen Sie sicher, dass die Dateipfade mit den Angaben in der Manifestdatei übereinstimmen.

- Eine Vorlagendatei enthält die AWS Ressourcen, die in Organisationseinheiten und Konten bereitgestellt werden sollen.
- Eine Richtliniendatei enthält die in der Vorlagendatei verwendeten Eingabeparameter.

Das folgende Beispiel zeigt die Ordnerstruktur für die in Schritt 1 erstellte Beispiel-Manifestdatei.

```
- manifest.yaml
- policies/
   - block-s3-public.json
- templates/
   - transit-gateway.template
```

Der 'Alfred'-Helfer und der CloudFormation Parameter-Dateien

CfCT bietet Ihnen einen Mechanismus, der als Alfred-Helfer bekannt ist, um den Wert für einen https://docs.aws.amazon.com/systems-manager/latest/userguide/systems-manager-parameter-store.html SSM-Parameterspeicherschlüssel abzurufen, der in der CloudFormation Vorlage definiert ist. Mit dem Alfred-Helper können Sie Werte verwenden, die im SSM-Parameterspeicher gespeichert sind, ohne die Vorlage zu aktualisieren. CloudFormation Weitere Informationen finden Sie unter Was ist eine CloudFormation Vorlage? im CloudFormation Benutzerhandbuch.

> **Important**
>
> Der Alfred-Helfer hat zwei Einschränkungen. Parameter sind nur in der Heimatregion des AWS Control Tower-Managementkontos verfügbar. Als bewährte Methode sollten Sie erwägen, mit Werten zu arbeiten, die sich von Stack-Instance zu Stack-Instance nicht ändern. Wenn der 'Alfred'-Helper Parameter abruft, wählt er eine zufällige Stack-Instanz aus dem Stack-Set aus, das die Variable exportiert.

Beispiel

Angenommen, Sie haben zwei CloudFormation Stack-Sets. Stack-Set 1 hat eine Stack-Instance und wird für ein Konto in einer Region bereitgestellt. Es erstellt eine Amazon-VPC und Subnetze in einer Verfügbarkeitszone. Diese `VPC ID` und `subnet ID` müssen als Parameterwerte an Stack-Set 2 übergeben werden. Bevor das `VPC ID` und an Stack-Set 2 übergeben werden *`subnet ID`* kann, `subnet ID` muss es `VPC ID` mithilfe von Stack-Set 1 gespeichert werden. `AWS:::SSM::Parameter` Weitere Informationen finden Sie unter `AWS:::SSM::Parameter` im CloudFormation -Benutzerhandbuch.

CloudFormation Stapelsatz 1:

Im folgenden Codeausschnitt kann der Alfred-Helper Werte für `VPC ID` und `subnet ID` aus dem Parameterspeicher abrufen und sie als Eingabe an die StackSet Zustandsmaschine übergeben.

```
VpcIdParameter:
    Type: AWS::SSM::Parameter
    Properties:
      Name: '/stack_1/vpc/id'
      Description: Contains the VPC id
      Type: String
```

```
      Value: !Ref MyVpc

SubnetIdParameter:
    Type: AWS::SSM::Parameter
    Properties:
      Name: '/stack_1/subnet/id'
      Description: Contains the subnet id
      Type: String
      Value: !Ref MySubnet
```

CloudFormation Stapelsatz 2:

Das Snippet zeigt die Parameter, die in der CloudFormation `manifest.yaml` Stack-2-Datei angegeben sind.

```
parameters:
      - parameter_key: VpcId
        parameter_value: $[alfred_ssm_/stack_1/vpc/id]
      - parameter_key: SubnetId
        parameter_value: $[alfred_ssm_/stack_1/subnet/id]
```

CloudFormation Stack-Set 2.1:

Das Snippet zeigt, dass Sie `alfred_ssm` Eigenschaften auflisten können, um Typparameter zu unterstützen. CommaDelimitedList Weitere Informationen finden Sie unter `Parameters` im CloudFormation -Benutzerhandbuch.

```
parameters:
      - parameter_key: VpcId # Type: String
        parameter_value: $[alfred_ssm_/stack_1/vpc/id']
      - parameter_key: SubnetId # Type: String
        parameter_value: $[ alfred_ssm_/stack_1/subnet/id']
      - parameter_key: AvailablityZones # Type: CommaDelimitedList
        parameter_value:
  - "$[alfred_ssm_/availability_zone_1]"
 - "$[alfred_ssm_/availability_zone_2]"
```

JSON-Schema für das Anpassungspaket

Das JSON-Schema für das Anpassungspaket für cFCT befindet sich im Quellcode-Repository unter GitHub. Sie können das Schema mit vielen Ihrer bevorzugten

Entwicklungstools verwenden. Möglicherweise finden Sie es hilfreich, um Fehler zu reduzieren, wenn Sie Ihre eigene `manifest.yaml` cFCT-Datei erstellen.

Versions-Upgrades für das cFCT-Manifest

Informationen zur neuesten Version von Customizations for AWS Control Tower (cFCT) finden Sie in der `CHANGELOG.md` Datei im Repository. GitHub

> **Warning**
>
> In Version 2.2.0 von Customizations for AWS Control Tower (cFCT) wurde ein cFCT-Manifestschema (Version 2021-03-15) eingeführt, das sich an den zugehörigen Service-APIs orientiert. AWS Das Manifestschema ermöglicht es einer einzigen manifest.yaml-Datei, unterstützte Ressourcen (CloudFormation Vorlagen, SCPs und RCPs) über entkoppelte Workflows zu verwalten. DevOps
> Wir empfehlen dringend, das cFCT-Manifestschema von Version 2020-01-01 auf Version 2021-03-15 oder höher zu aktualisieren.
> cFCT unterstützt weiterhin die Versionen 2021-03-15 und 2020-01-01 der Datei. `manifest.yaml` Es sind keine Änderungen an Ihrer bestehenden Konfiguration erforderlich. Für Version 2020-01-01 ist der Support jedoch abgelaufen. Wir bieten keine Updates mehr an oder fügen keine Verbesserungen mehr zu Version 2020-01-01 hinzu. Die Funktionen Root-OU und Nested OU werden in Version 2020-01-01 nicht unterstützt.

Veraltete Eigenschaften in der cFCT-Manifestversion 2021-03-15:

```
organization_policies
policy_file
apply_to_accounts_in_ou

cloudformation_resources
template_file
deploy_to_account
deploy_to_ou
ssm_parameters
```

Obligatorische cFCT-Upgrade-Schritte

Wenn Sie auf die Version 2021-03-15 des cFCT-Manifestschemas aktualisieren, müssen Sie folgende Änderungen vornehmen, um Ihre Dateien zu aktualisieren. In den nächsten Abschnitten werden die obligatorischen und empfohlenen Änderungen für den Übergang beschrieben.

Richtlinien der Organisationen

1. Verschieben Sie die SCPs oder RCPs unter organization_policies unter New Property Resources.
2. Ändern Sie die Eigenschaft policy_file in die neue Eigenschaft resource_file.
3. Ändern Sie die Eigenschaft apply_to_accounts_in_ou in die neue Eigenschaft deployment_targets. Die OU-Liste sollte unter der Untereigenschaft organizational_units definiert werden. Die Untereigenschaft accounts wird für Organisationsrichtlinien nicht unterstützt.
4. Fügen Sie eine neue Eigenschaft deploy_method mit dem Wert scp oder rcp hinzu.

CloudFormation Ressourcen

1. Verschieben Sie die CloudFormation Ressourcen unter cloudformation_resources unter neue Eigenschaftsressourcen.
2. Ändern Sie die Eigenschaft template_file in die neue Eigenschaft resource_file.
3. Ändern Sie die Eigenschaft deploy_to_ou in die neue Eigenschaft deployment_targets. Die OU-Liste sollte unter der Untereigenschaft organizational_units definiert werden.
4. Ändern Sie die Eigenschaft deploy_to_accounts in die neue Eigenschaft deployment_targets. Die Kontenliste sollte unter Untereigenschaftenkonten definiert werden.
5. Ändern Sie die Eigenschaft ssm_parameters in die neue Eigenschaft export_outputs.

Sehr empfehlenswerte cFCT-Upgrade-Schritte

CloudFormation Parameter

1. Ändern Sie die Eigenschaft parameter_file in neue Eigenschaftsparameter.
2. Entfernen Sie den Dateipfad im Wert der Eigenschaft parameter_file.
3. Kopieren Sie den Parameterschlüssel und den Parameterwert aus der vorhandenen Parameter-JSON-Datei in das neue Format für die Parametereigenschaft. Dies würde Ihnen helfen, sie in der Manifestdatei zu verwalten.

> **Note**
>
> Die Eigenschaft parameter_file wird in der cFCT-Manifestversion 2021-03-15 unterstützt.

Netzwerke im AWS Control Tower

AWS Control Tower bietet grundlegende Unterstützung für Netzwerke über VPCs.

Wenn die Standardkonfiguration oder die Funktionen der AWS Control Tower VPC Ihren Anforderungen nicht entsprechen, können Sie andere AWS Services verwenden, um Ihre VPC zu konfigurieren. Weitere Informationen zur Arbeit mit VPCs und AWS Control Tower finden Sie unter Aufbau einer skalierbaren und sicheren Multi-VPC AWS Netzwerkinfrastruktur.

AWS Control Tower unterstützt IPv4- und IPv6-Protokolle über Dual-Stack-IP-Adressen. Weitere Informationen finden Sie unter AWS Control Catalog-Endpunkte und Kontingente und AWS Control Tower-Endpunkte und Kontingente.

Verwandte Themen

- Informationen zur Funktionsweise von AWS Control Tower bei der Registrierung von Konten mit vorhandenen VPCs finden Sie unter. Registrieren Sie bestehende Konten bei VPCs
- Mit Account Factory können Sie Konten bereitstellen, die eine AWS Control Tower-VPC enthalten, oder Sie können Konten ohne VPC bereitstellen. Informationen zum Löschen der AWS Control Tower-VPC oder zum Konfigurieren von AWS Control Tower-Konten ohne VPC finden Sie unter. Exemplarische Vorgehensweise: Konfiguration des AWS Control Tower ohne VPC
- Informationen zum Ändern der Kontoeinstellungen für VPCs finden Sie in der Account Factory-Dokumentation zur Aktualisierung eines Kontos.
- Weitere Informationen zur Arbeit mit Netzwerken und VPCs in AWS Control Tower finden Sie im Abschnitt über Netzwerke auf der Seite mit verwandten Informationen in diesem Benutzerhandbuch.

VPCs und AWS Regionen im AWS Control Tower

Als Standardbestandteil der Kontoerstellung wird in jeder Region AWS eine Standard-VPC AWS erstellt, auch in den Regionen, die Sie nicht mit AWS Control Tower verwalten. Diese Standard-VPC ist nicht mit einer VPC identisch, die AWS Control Tower für ein bereitgestelltes Konto erstellt, aber die AWS Standard-VPC in einer Region ohne Verwaltung kann für IAM-Benutzer zugänglich sein.

Administratoren können die Option „Region verweigern“ aktivieren, sodass Ihre Endbenutzer nicht berechtigt sind, eine Verbindung zu einer VPC in einer Region herzustellen, die vom AWS

Control Tower unterstützt wird, aber außerhalb Ihrer regierten Regionen liegt. Um die Region Deny Control zu konfigurieren, gehen Sie zur Seite mit den Landingzone-Einstellungen und wählen Sie Einstellungen ändern aus.

Die Option „Region verweigern“ blockiert API-Aufrufe an die meisten Dienste ohne Steuerung. AWS-Regionen Weitere Informationen finden Sie unter Zugriff auf AWS basierend auf den angeforderten AWS-Region Daten verweigern. .

> **Note**
>
> Die Option Region Deny Control hindert IAM-Benutzer möglicherweise nicht daran, eine Verbindung zu einer AWS Standard-VPC in einer Region herzustellen, in der AWS Control Tower nicht unterstützt wird.

Optional können Sie die AWS Standard-VPCs in nicht regulierten Regionen entfernen. Um die Standard-VPC in einer Region aufzulisten, können Sie einen CLI-Befehl verwenden, der diesem Beispiel ähnelt:

```
aws ec2 --region us-west-1 describe-vpcs --filter Name=isDefault,Values=true
```

Überblick über AWS Control Tower und VPCs

Hier sind einige wichtige Fakten zu AWS Control Tower VPCs:

- Die von AWS Control Tower bei der Bereitstellung eines Kontos in Account Factory erstellte VPC ist nicht identisch mit der AWS Standard-VPC.
- AWS Control Tower löscht automatisch die Standard-VPC in Ihren ausgewählten regulierten Regionen (die AWS Regionen, die AWS Control Tower in Ihrer landing zone verwaltet) für Konten, die Sie über die AWS Control Tower Tower-Konsole erstellen. AWS Control Tower löscht die Standard-VPC in bestehenden Konten nicht. Dazu gehören Konten, die Sie in der `CreateLandingZone` Manifestdatei angeben oder die Sie während der Control Tower Tower-Einrichtung aus Ihrer AWS Organisation auswählen.
- Für jedes AWS Control Tower-Konto ist eine VPC zulässig, die von AWS Control Tower erstellt wurde. Ein Konto kann innerhalb des AWS Kontolimits zusätzliche VPCs haben.
- Jede AWS Control Tower VPC hat drei Availability Zones in allen Regionen außer der Region USA West (Nordkalifornien) und zwei Availability Zones in`us-west-1`. `us-west-1` Standardmäßig

werden jeder Availability Zone ein öffentliches Subnetz und zwei private Subnetze zugeteilt. Daher enthält jede AWS Control Tower Tower-VPC in Regionen mit Ausnahme der USA West (Nordkalifornien) standardmäßig neun Subnetze, die auf drei Availability Zones aufgeteilt sind. In USA West (Nordkalifornien) sind sechs Subnetze auf zwei Availability Zones aufgeteilt.

- Jedem der Subnetze in Ihrer AWS Control Tower VPC wird ein eindeutiger Bereich gleicher Größe zugewiesen.
- Die Anzahl der Subnetze in einer VPC ist konfigurierbar. Weitere Informationen zum Ändern der VPC-Subnetzkonfiguration finden Sie im Thema Account Factory.
- Da sich die IP-Adressen nicht überschneiden, können die sechs oder neun Subnetze innerhalb Ihrer AWS Control Tower VPC uneingeschränkt miteinander kommunizieren.

Bei der Arbeit mit VPCs macht AWS Control Tower keinen Unterschied auf regionaler Ebene. Jedem Subnetz wird genau aus dem CIDR-Bereich zugewiesen, den Sie angeben. Die VPC-Subnetze können in jeder Region vorhanden sein.

Hinweise

VPC-Kosten verwalten

Wenn Sie die Account Factory-VPC-Konfiguration so einrichten, dass öffentliche Subnetze bei der Bereitstellung eines neuen Kontos aktiviert werden, konfiguriert Account Factory VPC so, dass ein NAT-Gateway erstellt wird. Seine Nutzung wird Ihnen von Amazon VPC in Rechnung gestellt.

VPC- und Steuerungseinstellungen

Wenn Sie Account Factory Factory-Konten mit aktivierten VPC-Internetzugriffseinstellungen bereitstellen, hat diese Account Factory Factory-Einstellung Vorrang vor der Einstellung Internetzugriff verbieten für eine von einem Kunden verwaltete Amazon VPC-Instance. Um zu verhindern, dass der Internetzugang für neu bereitgestellte Konten aktiviert wird, müssen Sie die Einstellung in Account Factory ändern. Weitere Informationen finden Sie unter Exemplarische Vorgehensweise: Konfiguration von AWS Control Tower ohne VPC.

CIDR und Peering für VPC und AWS Control Tower

Dieser Abschnitt richtet sich in erster Linie an Netzwerkadministratoren. Der Netzwerkadministrator Ihres Unternehmens ist in der Regel die Person, die den gesamten CIDR-Bereich für Ihre AWS Control Tower Tower-Organisation auswählt. Der Netzwerkadministrator weist dann Subnetze aus diesem Bereich für bestimmte Zwecke zu.

Wenn Sie einen CIDR-Bereich für Ihre VPC auswählen, validiert AWS Control Tower die IP-Adressbereiche gemäß der RFC 1918-Spezifikation. Account Factory ermöglicht einen CIDR-Block von bis zu folgenden /16 Bereichen:

- `10.0.0.0/8`
- `172.16.0.0/12`
- `192.168.0.0/16`
- `100.64.0.0/10`(nur wenn Ihr Internetanbieter die Nutzung dieses Bereichs zulässt)

Das /16-Trennzeichen erlaubt bis zu 65 536 verschiedene IP-Adressen.

Sie können beliebige gültige IP-Adressen aus den folgenden Bereichen zuweisen:

- `10.0.x.x to 10.255.x.x`
- `172.16.x.x – 172.31.x.x`
- `192.168.0.0 – 192.168.255.255` (keine IPs außerhalb des `192.168`-Bereichs)

Wenn der von Ihnen angegebene Bereich außerhalb dieser Werte liegt, gibt AWS Control Tower eine Fehlermeldung aus.

Der Standard-CIDR-Bereich ist `172.31.0.0/16`.

Wenn AWS Control Tower eine VPC mit dem von Ihnen ausgewählten CIDR-Bereich erstellt, weist es jeder VPC für jedes Konto, das Sie innerhalb der Organisationseinheit (OU) erstellen, den identischen CIDR-Bereich zu. Aufgrund der standardmäßigen Überschneidung von IP-Adressen erlaubt diese Implementierung zunächst kein Peering zwischen Ihren AWS Control Tower Tower-VPCs in der Organisationseinheit.

Subnets

Innerhalb jeder VPC teilt AWS Control Tower Ihren angegebenen CIDR-Bereich gleichmäßig in neun Subnetze auf (außer in USA West (Nordkalifornien), wo es sich um sechs Subnetze handelt). Keines der Subnetze innerhalb einer VPC überschneidet sich. Daher können sie alle innerhalb der VPC miteinander kommunizieren.

Zusammenfassend lässt sich sagen, dass die Subnetzkommunikation innerhalb der VPC standardmäßig uneingeschränkt ist. Die bewährte Methode für die Steuerung der Kommunikation zwischen Ihren VPC-Subnetzen besteht bei Bedarf darin, Zugriffskontrolllisten mit Regeln einzurichten, die den zulässigen Datenfluss definieren. Verwenden Sie Sicherheitsgruppen für die Kontrolle des Datenverkehrs zwischen bestimmten Instances. Weitere Informationen zur Einrichtung von Sicherheitsgruppen und Firewalls in AWS Control Tower finden Sie unter Exemplarische Vorgehensweise: Sicherheitsgruppen in AWS Control Tower mit AWS Firewall Manager einrichten.

Peering

AWS Control Tower schränkt das VPC-to-VPC Peering für die Kommunikation zwischen mehreren VPCs nicht ein. Standardmäßig haben jedoch alle AWS Control Tower VPCs denselben Standard-CIDR-Bereich. Um Peering zu unterstützen, können Sie den CIDR-Bereich in den Einstellungen von Account Factory so ändern, dass sich die IP-Adressen nicht überschneiden.

Wenn Sie den CIDR-Bereich in den Einstellungen von Account Factory ändern, wird allen neuen Konten, die anschließend von AWS Control Tower (mithilfe von Account Factory) erstellt werden, der neue CIDR-Bereich zugewiesen. Die alten Konten werden nicht aktualisiert. Sie können beispielsweise ein Konto erstellen, dann den CIDR-Bereich ändern und ein neues Konto erstellen. Die VPCs, die diesen beiden Konten zugeordnet sind, können per Peering verbunden werden. Peering ist möglich, da ihre IP-Adressbereiche nicht identisch sind.

Greifen Sie über einen Schnittstellenendpunkt auf AWS Control Tower zu (AWS PrivateLink)

Sie können AWS PrivateLink es verwenden, um eine private Verbindung zwischen Ihrer VPC und dem AWS Control Tower herzustellen. Sie können auf den AWS Control Tower zugreifen, als ob er in Ihrer VPC wäre, ohne ein Internet-Gateway, ein NAT-Gerät, eine VPN-Verbindung oder Direct Connect eine Verbindung zu verwenden. Instances in Ihrer VPC benötigen keine öffentlichen IP-Adressen, um auf den AWS Control Tower zuzugreifen.

Sie stellen diese private Verbindung her, indem Sie einen Schnittstellen-Endpunkt erstellen, der von AWS PrivateLink unterstützt wird. Wir erstellen eine Endpunkt-Netzwerkschnittstelle in jedem

Subnetz, das Sie für den Schnittstellen-Endpunkt aktivieren. Dies sind vom Anforderer verwaltete Netzwerkschnittstellen, die als Einstiegspunkt für den Datenverkehr dienen, der für den AWS Control Tower bestimmt ist.

Weitere Informationen finden Sie AWS PrivateLink im Handbuch unter Access AWS-Services through. AWS PrivateLink

Überlegungen zu AWS Control Tower

Bevor Sie einen Schnittstellenendpunkt für AWS Control Tower einrichten, lesen Sie die Überlegungen im AWS PrivateLink Handbuch.

AWS Control Tower unterstützt das Aufrufen all seiner API-Aktionen über den Schnittstellenendpunkt.

Erstellen Sie einen Schnittstellenendpunkt für AWS Control Tower

Sie können einen Schnittstellenendpunkt für AWS Control Tower entweder mit der Amazon VPC-Konsole oder mit AWS Command Line Interface (AWS CLI) erstellen. Weitere Informationen finden Sie unter Erstellen eines Schnittstellenendpunkts im AWS PrivateLink -Leitfaden.

Erstellen Sie einen Schnittstellenendpunkt für AWS Control Tower mit den folgenden Servicenamen:

```
com.amazonaws.region.controltower
com.amazonaws.region.controltower-fips
```

Wenn Sie privates DNS für den Schnittstellenendpunkt aktivieren, können Sie API-Anfragen an den AWS Control Tower unter Verwendung des standardmäßigen regionalen DNS-Namens stellen. Beispiel, `controltower.us-east-1.amazonaws.com`.

Erstellen einer Endpunktrichtlinie für Ihren Schnittstellen-Endpunkt

Eine Endpunktrichtlinie ist eine IAM-Ressource, die Sie an einen Schnittstellen-Endpunkt anfügen können. Die Standard-Endpunktrichtlinie ermöglicht den vollen Zugriff auf den AWS Control Tower über den Schnittstellenendpunkt. Um den Zugriff auf AWS Control Tower von Ihrer VPC aus zu kontrollieren, fügen Sie dem Schnittstellenendpunkt eine benutzerdefinierte Endpunktrichtlinie hinzu.

Eine Endpunktrichtlinie gibt die folgenden Informationen an:

- Die Prinzipale, die Aktionen ausführen können (AWS-Konten, IAM-Benutzer und IAM-Rollen).
- Aktionen, die ausgeführt werden können

- Die Ressourcen, auf denen die Aktionen ausgeführt werden können.

Weitere Informationen finden Sie unter Steuern des Zugriffs auf Services mit Endpunktrichtlinien im AWS PrivateLink -Leitfaden.

Beispiel: VPC-Endpunktrichtlinie für AWS Control Tower-Aktionen

Im Folgenden finden Sie ein Beispiel für eine benutzerdefinierte Endpunktrichtlinie. Wenn Sie diese Richtlinie an Ihren Schnittstellenendpunkt anhängen, gewährt sie allen Prinzipalen auf allen Ressourcen Zugriff auf die aufgelisteten AWS Control Tower-Aktionen.

```
{
   "Statement": [
      {
         "Principal": "*",
         "Effect": "Allow",
         "Action": [
            "controltower:ListEnabledControls",
            "controltower:ListLandingZones"
         ],
         "Resource":"*"
      }
   ]
}
```

> **Note**
>
> Eine vollständige Liste der AWS Control Tower-API-Operationen finden Sie in der AWS Control Tower API-Referenz.

Erforderliche Rollen und Berechtigungen

AWS Control Tower verwendet IAM-Rollen, um den Zugriff auf Ressourcen zu verwalten.

Allgemeine Informationen zu Rollen finden Sie unter Benutzergruppen, Rollen und Berechtigungssätze.

Berechtigungen

- Informationen zu IAM-Gruppen und ihren Berechtigungen in AWS Control Tower finden Sie unter IAM Identity Center-Gruppen für AWS Control Tower.
- Informationen zu den für die Bereitstellung von Konten erforderlichen Berechtigungen finden Sie unter Erforderliche Berechtigungen für Konten.
- Informationen zu den für AWS Control Tower erforderlichen Konsolenberechtigungen finden Sie unter Erforderliche Berechtigungen für die Nutzung der AWS Control Tower Tower-Konsole.

Über Rollen

- Informationen zum Erstellen einer Rolle, einschließlich der für den programmatischen Zugriff vorgesehenen Berechtigungen, finden Sie unter Rollen erstellen und Berechtigungen zuweisen und Programmgesteuerte Rollen und Vertrauensbeziehungen für das AWS Control Tower Tower-Auditkonto.
- Informationen zu anderen Rollen, die AWS Control Tower zur Verwaltung Ihrer Konten verwendet, finden Sie unter Verwenden von identitätsbasierten Richtlinien (IAM-Richtlinien) für AWS Control Tower und unter Verwaltete Richtlinien für AWS Control Tower.
- Informationen zu AWS Control Tower und AWS Config Rollen finden Sie unter AWS Control Tower ConfigRecorderRole.
- Informationen zu Rollen, die AWS Control Tower verwendet, um AWS Config Informationen für Ihre Konten zu aggregieren, finden Sie unter So aggregiert AWS Control Tower AWS Config Regeln in nicht verwalteten Organisationseinheiten und Konten.
- Informationen zum Schutz Ihrer Ressourcen bei der Zuweisung von Rollen und Berechtigungen finden Sie unter Optionale Bedingungen für Ihre Rollenvertrauensbeziehungen, Optionale Konfiguration von AWS KMS Schlüsseln und Verhinderung von dienstübergreifendem Identitätswechsel.
- Spezifische Informationen zur automatisierten Kontobereitstellung in AWS Control Tower mit IAM-Rollen finden Sie unter Automatisierte Kontobereitstellung mit IAM-Rollen.

- Die Richtlinie zum Schutz des SNS-Themas finden Sie unter Die AWS Config SNS-Themenrichtlinie. AWS Config

So funktioniert AWS Control Tower mit Rollen zur Erstellung und Verwaltung von Konten

Im Allgemeinen sind Rollen Teil des Identitäts- und Zugriffsmanagements (IAM) in AWS. Allgemeine Informationen zu IAM und Rollen in AWS finden Sie unter dem Thema IAM-Rollen im AWS IAM-Benutzerhandbuch.

Rollen und Kontoerstellung

AWS Control Tower erstellt ein Kundenkonto, indem es die `CreateAccount` API von aufruft AWS Organizations. Bei AWS Organizations der Erstellung dieses Kontos wird eine Rolle innerhalb dieses Kontos erstellt, die AWS Control Tower benennt, indem ein Parameter an die API übergeben wird. Der Name der Rolle lautet `AWSControlTowerExecution`.

AWS Control Tower übernimmt die `AWSControlTowerExecution` Rolle für alle Konten, die von Account Factory erstellt wurden. Mithilfe dieser Rolle erstellt AWS Control Tower ein Baselining für das Konto und wendet obligatorische (und alle anderen aktivierten) Kontrollen an, was zur Erstellung weiterer Rollen führt. Diese Rollen werden wiederum von anderen Diensten verwendet, wie z. AWS Config

> **Note**
>
> Um ein Konto als Baseline zu definieren, müssen die zugehörigen Ressourcen eingerichtet werden. Dazu gehören Account Factory Factory-Vorlagen, die manchmal auch als Blueprints bezeichnet werden, und Kontrollen. Im Rahmen des Baselining-Prozesses werden im Rahmen der Bereitstellung der Vorlagen auch die zentralen Rollen für Protokollierung und Sicherheitsprüfung für das Konto eingerichtet. Die AWS Control Tower Tower-Baselines sind in den Rollen enthalten, die Sie für jedes registrierte Konto anwenden.

Weitere Informationen zu Konten und Ressourcen finden Sie unter. Informationen AWS-Konten im AWS Control Tower

Die AWSControlTowerExecution Rolle, erklärt

Die Rolle `AWSControlTowerExecution` muss in allen angemeldeten Konten vorhanden sein. Es ermöglicht AWS Control Tower, Ihre individuellen Konten zu verwalten und Informationen darüber an Ihre Audit- und Log Archive-Konten zu melden.

Die `AWSControlTowerExecution` Rolle kann einem Konto auf verschiedene Weise hinzugefügt werden, und zwar wie folgt:

- Für Konten in der Security OU (manchmal auch als Kernkonten bezeichnet) erstellt AWS Control Tower die Rolle bei der ersten Einrichtung von AWS Control Tower.
- Für ein Account Factory Factory-Konto, das über die AWS Control Tower-Konsole erstellt wurde, erstellt AWS Control Tower diese Rolle zum Zeitpunkt der Kontoerstellung.
- Für die Registrierung eines einzelnen Kontos bitten wir Kunden, die Rolle manuell zu erstellen und das Konto dann bei AWS Control Tower zu registrieren.
- Wenn die Steuerung auf eine Organisationseinheit ausgedehnt wird, verwendet AWS Control Tower die StackSet-AWSControlTowerExecutionRole, um die Rolle in allen Konten in dieser Organisationseinheit zu erstellen.

> **Note**
>
> Wenn Sie ein Konto abmelden, entfernt AWS Control Tower die `AWSControlTowerExecution` Rolle, unabhängig davon, ob sie manuell oder von AWS Control Tower selbst erstellt wurde.

Zweck der `AWSControlTowerExecution` Rolle:

- `AWSControlTowerExecution`ermöglicht es Ihnen, Konten automatisch mit Skripten und Lambda-Funktionen zu erstellen und zu registrieren.
- `AWSControlTowerExecution` hilft Ihnen bei der Konfiguration der Protokollierung Ihrer Organisationen, sodass alle Protokolle für jedes Konto an das Protokollierungskonto gesendet werden.
- `AWSControlTowerExecution`ermöglicht es Ihnen, ein individuelles Konto bei AWS Control Tower zu registrieren. Zunächst müssen Sie die `AWSControlTowerExecution` Rolle zu

diesem Konto hinzufügen. Anweisungen zum Hinzufügen der Rolle finden Sie unterFügen Sie die erforderliche IAM-Rolle manuell zu einer vorhandenen hinzu AWS-Konto und registriere es.

So funktioniert die `AWSControlTowerExecution` Rolle mit Organisationseinheiten:

Die `AWSControlTowerExecution` Rolle stellt sicher, dass Ihre ausgewählten AWS Control Tower-Kontrollen automatisch für jedes einzelne Konto in jeder Organisationseinheit in Ihrer Organisation sowie für jedes neue Konto gelten, das Sie in AWS Control Tower erstellen. Das Ergebnis:

- Auf der Grundlage der Prüf- und Protokollierungsfunktionen von AWS Control Tower Controls können Sie Compliance- und Sicherheitsberichte einfacher bereitstellen.
- Ihre Sicherheits- und Compliance-Teams können überprüfen, ob alle Anforderungen erfüllt sind und keine Abweichungen bzgl. der Organisation aufgetreten sind.

Weitere Informationen zu Drift finden Sie unter Drift erkennen und beheben in AWS Control Tower.

Zusammenfassend lässt sich sagen, dass die `AWSControlTowerExecution`-Rolle und ihre zugehörigen Richtlinien Ihnen eine flexible Kontrolle der Sicherheit und der Einhaltung von Vorschriften in Ihrer gesamten Organisation ermöglichen. Daher ist es weniger wahrscheinlich, dass es zu Sicherheits- oder Protokollverstößen kommt.

Optionale Bedingungen für Ihre Rolle, Ihre Vertrauensbeziehungen

Um Ihrer AWS Control Tower-Umgebung zusätzliche Sicherheitsebenen hinzuzufügen, können Sie in Ihren Richtlinien zur Rollenvertrauensstellung Bedingungen festlegen, um die Konten und Ressourcen einzuschränken, die mit bestimmten Rollen in AWS Control Tower interagieren. Sie können beispielsweise den Zugriff auf die `AWSControlTowerAdmin` Rolle weiter einschränken, da sie umfassende Zugriffsberechtigungen ermöglicht.

Um zu verhindern, dass ein Bedrohungsakteur Zugriff auf Ihre Ressourcen erhält, bearbeiten Sie Ihre AWS Control Tower Tower-Vertrauensrichtlinie manuell, um der Richtlinienerklärung mindestens eine `aws:SourceArn` oder eine `aws:SourceAccount` Bedingung hinzuzufügen. Als zusätzliche bewährte Sicherheitsmethode können Sie die `aws:SourceArn` Bedingung hinzufügen, da sie spezifischer ist als `aws:SourceAccount` die Beschränkung des Zugriffs auf ein bestimmtes Konto und eine bestimmte Ressource.

Wenn Sie den vollständigen ARN der Ressource nicht kennen oder wenn Sie mehrere Ressourcen angeben, können Sie die `aws:SourceArn` Bedingung mit Platzhaltern (*) für die unbekannten Teile

des ARN verwenden. `arn:aws:controltower:*:123456789012:*`Funktioniert beispielsweise, wenn Sie keine Region angeben möchten.

Das folgende Beispiel zeigt die Verwendung der `aws:SourceArn` IAM-Bedingung mit den Vertrauensrichtlinien Ihrer IAM-Rolle. Fügen Sie die Bedingung in Ihrer Vertrauensbeziehung für die AWSControlTowerAdminRolle hinzu, da der AWS Control Tower Service Principal mit ihr interagiert.

Wie im Beispiel gezeigt, hat der Quell-ARN das folgende Format: `arn:aws:controltower:${HOME_REGION}:${CUSTOMER_AWSACCOUNT_id}:*`

Ersetzen Sie die Zeichenfolgen `${HOME_REGION}` und `${CUSTOMER_AWSACCOUNT_id}` durch Ihre eigene Heimatregion und die Konto-ID des anrufenden Kontos.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "controltower.amazonaws.com"
        ]
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "ArnEquals": {
          "aws:SourceArn": "arn:aws:controltower:us-west-2:012345678901:*"
        }
      }
    }
  ]
}
```

In diesem Beispiel `arn:aws:controltower:us-west-2:012345678901:*` ist der als angegebene Quell-ARN der einzige ARN, der die `sts:AssumeRole` Aktion ausführen darf. Mit anderen Worten, nur Benutzer, die sich mit der Konto-ID `012345678901` in der `us-west-2` Region anmelden können, dürfen Aktionen ausführen, die diese spezielle Rolle und Vertrauensbeziehung für den AWS Control Tower Tower-Service erfordern, benannt als`controltower.amazonaws.com`.

Das nächste Beispiel zeigt die `aws:SourceArn` Bedingungen `aws:SourceAccount` und Bedingungen, die für die Vertrauensrichtlinie für Rollen gelten.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "controltower.amazonaws.com"
        ]
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "012345678901"
        },
        "ArnLike": {
          "aws:SourceArn": "arn:aws:controltower:us-west-2:012345678901:*"
        }
      }
    }
  ]
}
```

Das Beispiel veranschaulicht die `aws:SourceArn` Bedingungsanweisung mit einer zusätzlichen `aws:SourceAccount` Bedingungsanweisung. Weitere Informationen finden Sie unter Verhindern Sie dienstübergreifenden Identitätswechsel.

Allgemeine Informationen zu Berechtigungsrichtlinien in AWS Control Tower finden Sie unterVerwalte den Zugriff auf Ressourcen.

Empfehlungen:

Wir empfehlen, den Rollen, die AWS Control Tower erstellt, Bedingungen hinzuzufügen, da diese Rollen direkt von anderen AWS-Services übernommen werden. Weitere Informationen finden Sie in dem Beispiel für AWSControlTowerAdmin, das zuvor in diesem Abschnitt gezeigt wurde. Für die

AWS Config Recorder-Rolle empfehlen wir, die `aws:SourceArn` Bedingung hinzuzufügen und den Config-Recorder-ARN als zulässigen Quell-ARN anzugeben.

Für Rollen wie AWSControlTowerExecutionoder andere programmatische Rollen, die vom AWS Control Tower Audit-Konto in allen verwalteten Konten übernommen werden können, empfehlen wir, die `aws:PrincipalOrgID` Bedingung zur Vertrauensrichtlinie für diese Rollen hinzuzufügen, wodurch bestätigt wird, dass der Principal, der auf die Ressource zugreift, zu einem Konto in der richtigen AWS Organisation gehört. Fügen Sie die `aws:SourceArn` Bedingungsanweisung nicht hinzu, da sie nicht wie erwartet funktionieren wird.

> **Note**
>
> Im Falle einer Abweichung ist es möglich, dass eine AWS Control Tower Tower-Rolle unter bestimmten Umständen zurückgesetzt wird. Es wird empfohlen, die Rollen regelmäßig erneut zu überprüfen, falls Sie sie angepasst haben.

So aggregiert AWS Control Tower AWS Config Regeln in nicht verwalteten Organisationseinheiten und Konten

- Das AWS Control Tower-Verwaltungskonto erstellt einen Aggregator auf Organisationsebene, der bei der Erkennung externer AWS Config Regeln hilft, sodass AWS Control Tower keinen Zugriff auf nicht verwaltete Konten erhalten muss. Die AWS Control Tower Tower-Konsole zeigt Ihnen, wie viele extern erstellte AWS Config Regeln Sie für ein bestimmtes Konto haben. Sie können Details zu diesen externen Regeln auf der Registerkarte Einhaltung externer Konfigurationsregeln auf der Seite mit den Kontodetails anzeigen.
- Um den Aggregator zu erstellen, fügt AWS Control Tower eine Rolle mit den erforderlichen Berechtigungen hinzu, um eine Organisation zu beschreiben und die ihr untergeordneten Konten aufzulisten. Die `AWSControlTowerConfigAggregatorRoleForOrganizations` Rolle erfordert die `AWSConfigRoleForOrganizations` verwaltete Richtlinie und eine Vertrauensbeziehung mit`config.amazonaws.com`.

> **Note**
>
> Kunden, die landing zone Version 4.0 verwenden, benötigen diese Rolle nicht, da AWS Control Tower vom bestehenden Konfigurationsaggregator auf Organisationsebene zum serviceverknüpften Konfigurationsaggregator migriert ist.

> **Note**
>
> Wenn Sie vertrauenswürdigen Zugriff für die Organisation aktivieren, die Ihre landing zone enthält, kann AWS Control Tower Rollen erstellen, Ressourcen verwalten und Daten für alle Konten in der Organisation lesen. Durch vertrauenswürdigen Zugriff steht AWS Control Tower jedes Konto oder jede Organisationseinheit in der Organisation zur Verfügung, unabhängig davon, ob es registriert und registriert oder nicht registriert und nicht registriert ist.

Hier ist die IAM-Richtlinie (JSON-Artefakt), die der Rolle zugeordnet ist:

JSON

```
{
    "Version":"2012-10-17",
      "Statement": [
       {
        "Effect": "Allow",
        "Action": [
          "organizations:ListAccounts",
          "organizations:DescribeOrganization",
          "organizations:ListAWSServiceAccessForOrganization"
         ],
       "Resource": "*"
      }
    ]
  }
```

Hier ist die `AWSControlTowerConfigAggregatorRoleForOrganizations` Vertrauensbeziehung:

```
{
    "Version": "2012-10-17",
      "Statement": [
      {
        "Effect": "Allow",
        "Principal": {
        "Service": "config.amazonaws.com"
        },
        "Action": "sts:AssumeRole"
      }
    ]
  }
}
```

Um diese Funktionalität im Verwaltungskonto bereitzustellen, werden der verwalteten RichtlinieAWSControlTowerServiceRolePolicy, die von der AWSControlTowerAdmin Rolle bei der Erstellung des AWS Config Aggregators verwendet wird, die folgenden Berechtigungen hinzugefügt:

JSON

```
{
  "Version":"2012-10-17",
    "Statement": [
      {
        "Effect": "Allow",
        "Action": [
          "config:PutConfigurationAggregator",
          "config:DeleteConfigurationAggregator",
          "iam:PassRole"
          ],
        "Resource": [
          "arn:aws:iam::123456789012:role/service-role/
AWSControlTowerConfigAggregatorRoleForOrganizations",
          "arn:aws:config:us-east-1:123456789012:config-aggregator/"
          ]
        },
      {
        "Effect": "Allow",
        "Action": "organizations:EnableAWSServiceAccess",
        "Resource": "*"
```

```
      }
    ]
}
```

Neue Ressourcen wurden erstellt: `AWSControlTowerConfigAggregatorRoleForOrganizations` und `aws-controltower-ConfigAggregatorForOrganizations`

Wenn Sie bereit sind, können Sie Konten einzeln oder als Gruppe registrieren, indem Sie eine Organisationseinheit registrieren. Wenn Sie ein Konto registriert haben und eine Regel in erstellen AWS Config, erkennt AWS Control Tower die neue Regel. Der Aggregator zeigt die Anzahl der externen Regeln an und bietet einen Link zur AWS Config Konsole, über die Sie die Details jeder externen Regel für Ihr Konto einsehen können. Ermitteln Sie anhand der Informationen in der AWS Config Konsole und der AWS Control Tower Tower-Konsole, ob Sie die entsprechenden Kontrollen für das Konto aktiviert haben.

Programmgesteuerte Rollen und Vertrauensbeziehungen für das AWS Control Tower Tower-Auditkonto

Sie können sich beim Auditkonto anmelden und programmgesteuert die Rolle übernehmen, andere Konten zu überprüfen. Das Prüfungskonto erlaubt Ihnen nicht, sich manuell bei anderen Konten anzumelden.

Das Auditkonto ermöglicht Ihnen mithilfe einiger Rollen, die nur AWS Lambda-Funktionen gewährt werden, programmatischen Zugriff auf andere Konten. Aus Sicherheitsgründen haben diese Rollen Vertrauensbeziehungen zu anderen Rollen, was bedeutet, dass die Bedingungen, unter denen die Rollen verwendet werden können, genau definiert sind.

Der AWS Control Tower Tower-Stack `StackSet-AWSControlTowerBP-BASELINE-ROLES` erstellt diese ausschließlich programmgesteuerten, kontoübergreifenden IAM-Rollen in jedem verwalteten Konto, einschließlich des Config-Aggregator-Kontos (früher das Auditkonto). Das Config-Aggregator-Konto übernimmt diese Ausführungsrollen, um programmgesteuert auf andere Konten zuzugreifen:

- aws-controltower- AdministratorExecutionRole
- aws-Kontrollturm- ReadOnlyExecutionRole

Der AWS Control Tower Tower-Stack `StackSet-AWSControlTowerSecurityResources` erstellt diese ausschließlich programmgesteuerten, kontoübergreifenden IAM-Rollen im Auditkonto:

- aws-controltower- AuditAdministratorRole
- aws-Kontrollturm- AuditReadOnlyRole

`ReadOnlyExecutionRole:`Beachten Sie, dass diese Rolle es dem Auditkonto ermöglicht, Objekte in Amazon S3 S3-Buckets in der gesamten Organisation zu lesen (im Gegensatz zu der `SecurityAudit` Richtlinie, die nur den Zugriff auf Metadaten zulässt).

aws-controltower-: AdministratorExecutionRole

- Hat Administratorrechte
- Kann von der Konsole aus nicht angenommen werden
- Kann nur von einer Rolle im Auditkonto übernommen werden — dem `aws-controltower-AuditAdministratorRole`

Das folgende Artefakt zeigt das Vertrauensverhältnis für`aws-controltower-AdministratorExecutionRole`. Die Platzhalternummer `012345678901` wird durch die `Audit_acct_ID` Nummer für Ihr Auditkonto ersetzt.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::012345678901:role/aws-controltower-AuditAdministratorRole"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

aws-controltower-: AuditAdministratorRole

- Kann nur vom AWS Lambda-Service übernommen werden
- Hat die Berechtigung, Lese- (Get) und Schreibvorgänge (Put) für Amazon S3 S3-Objekte durchzuführen, deren Namen mit der Zeichenfolge log beginnen

Beigefügte Richtlinien:

1. AWSLambdaExecute— AWS verwaltete Richtlinie

2. AssumeRole-aws-controltower-AuditAdministratorRole— Inline-Richtlinie — Erstellt von AWS Control Tower, Artifact folgt.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
 {
 "Action": [
   "sts:AssumeRole"
   ],
 "Resource": [
   "arn:aws:iam::*:role/aws-controltower-AdministratorExecutionRole"
   ],
 "Effect": "Allow"
 }
   ]
}
```

Das folgende Artefakt zeigt die Vertrauensbeziehung für: `aws-controltower-AuditAdministratorRole`

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "lambda.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

aws-controltower-: ReadOnlyExecutionRole

- Kann von der Konsole aus nicht angenommen werden

- Kann nur von einer anderen Rolle im Auditkonto übernommen werden — der `AuditReadOnlyRole`

Das folgende Artefakt zeigt das Vertrauensverhältnis für`aws-controltower-ReadOnlyExecutionRole`. Die Platzhalternummer `012345678901` wird durch die `Audit_acct_ID` Nummer für Ihr Auditkonto ersetzt.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::012345678901:role/aws-controltower-AuditReadOnlyRole "
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

aws-controltower-: AuditReadOnlyRole

- Kann nur vom AWS Lambda-Service übernommen werden
- Hat die Berechtigung, Lese- (Get) und Schreibvorgänge (Put) für Amazon S3 S3-Objekte durchzuführen, deren Namen mit der Zeichenfolge log beginnen

Beigefügte Richtlinien:

1. AWSLambdaExecute— AWS verwaltete Richtlinie

2. AssumeRole-aws-controltower-AuditReadOnlyRole— Inline-Richtlinie — Erstellt von AWS Control Tower, Artifact folgt.

JSON

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

```
 "Action": [
  "sts:AssumeRole"
 ],
 "Resource": [
  "arn:aws:iam::*:role/aws-controltower-ReadOnlyExecutionRole"
 ],
 "Effect": "Allow"
   }
  ]
}
```

Das folgende Artefakt zeigt die Vertrauensbeziehung für: `aws-controltower-AuditReadOnlyRole`

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "lambda.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Automatisierte Kontobereitstellung mit IAM-Rollen

Um Account Factory Factory-Konten automatisierter zu konfigurieren, können Sie Lambda-Funktionen im AWS Control Tower Tower-Verwaltungskonto erstellen, das die AWSControlTowerExecutionRolle im Mitgliedskonto übernimmt. Anschließend führt das Verwaltungskonto mithilfe der Rolle die gewünschten Konfigurationsschritte in jedem Mitgliedskonto durch.

Wenn Sie Konten mithilfe von Lambda-Funktionen bereitstellen, muss die Identität, die diese Arbeit ausführt, zusätzlich zu die folgende IAM-Berechtigungsrichtlinie aufweisen. `AWSServiceCatalogEndUserFullAccess`

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSControlTowerAccountFactoryAccess",
            "Effect": "Allow",
            "Action": [
                "sso:GetProfile",
                "sso:CreateProfile",
                "sso:UpdateProfile",
                "sso:AssociateProfile",
                "sso:CreateApplicationInstance",
                "sso:GetSSOStatus",
                "sso:GetTrust",
                "sso:CreateTrust",
                "sso:UpdateTrust",
                "sso:GetApplicationInstance",
                "sso:ListDirectoryAssociations",
                "sso:ListPermissionSets",
                "sso:GetPermissionSet",
                "sso:ListProfileAssociations",
                "sso-directory:ListMembersInGroup",
                "sso-directory:AddMemberToGroup",
                "sso-directory:SearchGroups",
                "sso-directory:SearchUsers",
                "sso-directory:CreateUser",
                "sso-directory:DescribeGroups",
                "sso-directory:DescribeDirectory",
                "sso-directory:GetUserPoolInfo",
                "controltower:CreateManagedAccount",
                "controltower:DescribeManagedAccount",
                "controltower:DeregisterManagedAccount",
                "s3:GetObject",
                "organizations:describeOrganization",
                "sso:DescribeRegisteredRegions"
            ],
            "Resource": "*"
        }
    ]
}
```

Ressourcen im AWS Control Tower

- Allgemeine Informationen zum Ressourcenbesitz in AWS Control Tower finden Sie unterÜberblick über die Verwaltung von Zugriffsberechtigungen für Ihre AWS Control Tower-Ressourcen.
- Informationen zu Ressourcen, die AWS Control Tower in den gemeinsamen Konten erstellt, finden Sie unterKonten zur Serviceintegration.
- Informationen zu Ressourcen, die AWS Control Tower bei der Bereitstellung eines Kontos über Account Factory erstellt, finden Sie unterÜberlegungen zu Ressourcen für Account Factory.
- Einzelheiten zu den AWS Ressourcentypen, die von AWS Control Tower zur Verwendung mit den AWS Control Tower Tower-APIs definiert wurden, finden Sie in der AWS Control Tower Tower-Ressourcentyp-Referenz im AWS CloudFormation Benutzerhandbuch.

Wie AWS Regionen arbeiten mit AWS Control Tower

AWS Control Tower wird in den folgenden AWS Regionen unterstützt:

- USA Ost (Nord-Virginia)
- USA Ost (Ohio)
- USA West (Oregon)
- Kanada (Zentral)
- Asien-Pazifik (Sydney)
- Asien-Pazifik (Singapur)
- Europe (Frankfurt)
- Europa (Irland)
- Europe (London)
- Europa (Stockholm)
- Asien-Pazifik (Mumbai)
- Asia Pacific (Seoul)
- Asien-Pazifik (Tokio)
- Europa (Paris)
- Südamerika (São Paulo)
- USA West (Nordkalifornien)
- Asien-Pazifik (Hongkong)
- Asien-Pazifik (Jakarta)
- Asien-Pazifik (Osaka)
- Europa (Milan)
- Afrika (Kapstadt)
- Middle East (Bahrain)
- Israel (Tel Aviv)
- Naher Osten (VAE)
- Europa (Spain)

- Asien-Pazifik (Hyderabad)
- Europa (Zürich)
- Asien-Pazifik (Melbourne)
- Kanada West (Calgary)
- Malaysien (Kuala Lumpur)
- Asien-Pazifik (Thailand)
- Mexiko (Zentral)
- Asien-Pazifik (Taipeh)

Über deine Heimatregion

Wenn Sie eine Landing Zone erstellen, wird die Region, die Sie für den Zugriff auf die AWS Management Console verwenden, zu Ihrer AWS Heimatregion für AWS Control Tower. Während des Erstellungsprozesses werden einige Ressourcen in der Heimatregion bereitgestellt. Andere Ressourcen, wie Organisationseinheiten und AWS Konten, sind global.

Nachdem Sie eine Heimatregion ausgewählt haben, können Sie sie nicht mehr ändern.

Steuerungen und Regionen

Derzeit funktionieren alle präventiven Kontrollen weltweit. Detektive und proaktive Kontrollen funktionieren jedoch nur in Regionen, in denen AWS Control Tower unterstützt wird. Weitere Informationen zum Verhalten von Steuerungen bei der Aktivierung von AWS Control Tower in einer neuen Region finden Sie unterKonfigurieren Sie Ihre AWS Control Tower-Regionen.

Konfigurieren Sie Ihre AWS Control Tower-Regionen

In diesem Abschnitt wird das Verhalten beschrieben, das Sie erwarten können, wenn Sie Ihre AWS Control Tower-Landing Zone auf eine neue AWS Region erweitern oder eine Region aus Ihrer Landing Zone-Konfiguration entfernen. Im Allgemeinen wird diese Aktion über die Aktualisierungsfunktion der AWS Control Tower-Konsole ausgeführt.

> **Note**
>
> Wir empfehlen Ihnen, Ihre AWS Control Tower-Landezone nicht auf AWS Regionen auszudehnen, in denen Ihre Workloads nicht ausgeführt werden müssen. Wenn Sie sich

von einer Region abmelden, hindert Sie das nicht daran, Ressourcen in dieser Region bereitzustellen, aber diese Ressourcen bleiben außerhalb der Verwaltung von AWS Control Tower.

Während der Konfiguration einer neuen Region aktualisiert der AWS Control Tower die Landezone, was bedeutet, dass sie als Basislinie für Ihre Landezone dient —

- in allen neu ausgewählten Regionen aktiv zu agieren und
- die Verwaltung der Ressourcen in den ausgewählten Regionen einzustellen.

Einzelne Konten innerhalb Ihrer Organisationseinheiten (OUs), die vom AWS Control Tower verwaltet werden, werden im Rahmen dieser Aktualisierung der Landezone nicht aktualisiert. Daher müssen Sie Ihre Konten aktualisieren, indem Sie Ihre OUs erneut registrieren.

Beachten Sie bei der Konfiguration Ihrer AWS Control Tower-Regionen die folgenden Empfehlungen und Einschränkungen:

- Wählen Sie Regionen aus, in denen Sie AWS Ressourcen oder Workloads hosten möchten.
- Wenn Sie sich von einer Region abmelden, werden Sie nicht daran gehindert, Ressourcen in dieser Region bereitzustellen, aber diese Ressourcen bleiben außerhalb der Verwaltung von AWS Control Tower.

Wenn Sie Ihre Landezone für neue Regionen konfigurieren, halten sich die Detektivkontrollen von AWS Control Tower an die folgenden Regeln:

- Was vorhanden ist, bleibt gleich. Das Kontrollverhalten, sowohl detektivisch als auch präventiv, bleibt für bestehende Konten, in bestehenden Organisationseinheiten und in bestehenden Regionen unverändert.
- Sie können keine neuen Detektivkontrollen auf bestehende Organisationseinheiten anwenden, die Konten enthalten, die nicht aktualisiert wurden. Wenn Sie Ihre AWS Control Tower-Landing Zone für eine neue Region konfiguriert haben (indem Sie Ihre Landing Zone aktualisieren), müssen Sie die vorhandenen Konten in Ihren vorhandenen OUs aktualisieren, bevor Sie neue Detective Controls für diese OUs und Konten aktivieren können.
- Ihre bestehenden Detective Controls beginnen in den neu konfigurierten Regionen zu funktionieren, sobald Sie die Konten aktualisieren. Wenn Sie Ihre AWS Control Tower-Landing

Zone aktualisieren, um neue Regionen zu konfigurieren, und dann ein Konto aktualisieren, beginnen die Detective Controls, die bereits in der OU aktiviert sind, auf diesem Konto in den neu konfigurierten Regionen zu arbeiten.

Konfigurieren Sie die AWS Control Tower-Regionen

1. Melden Sie sich bei der AWS Control Tower-Konsole unter an https://console.aws.amazon.com/controltower
2. Wählen Sie im linken Navigationsmenü die Option Landing Zone Settings aus.
3. Wählen Sie auf der Seite mit den Landingzone-Einstellungen im Abschnitt Details oben rechts die Schaltfläche Einstellungen ändern aus. Sie werden zum Workflow „Landing Zone aktualisieren“ weitergeleitet.
4. Suchen Sie unter Zusätzliche verwaltete Regionen nach den Regionen, die Sie regieren möchten (oder beenden) möchten.
5. Markieren Sie das Kontrollkästchen für jede weitere Region, die Sie regeln möchten. Deaktivieren Sie das Kontrollkästchen für jede Region, aus der Sie die Unternehmensführung entfernen möchten.

> **Note**
>
> Wenn Sie sich dafür entscheiden, eine Region nicht zu verwalten, können Sie weiterhin Ressourcen in dieser Region bereitstellen, aber diese Ressourcen bleiben außerhalb der Verwaltung durch AWS Control Tower.

6. Schließen Sie den Rest des Workflows ab und wählen Sie dann Landing Zone aktualisieren.
7. Wenn die Einrichtung der Landing Zone abgeschlossen ist, Re-register verwenden Sie die OUs, um die Konten in Ihren neuen Regionen zu aktualisieren. Weitere Informationen finden Sie unter Wann sollten die Organisationseinheiten und Konten von AWS Control Tower aktualisiert werden.

Eine alternative Methode zur Bereitstellung oder Aktualisierung einzelner Konten nach der Konfiguration neuer Regionen besteht darin, das API-Framework von Service Catalog AWS CLI zu verwenden und die Konten in einem Batch-Prozess zu aktualisieren. Weitere Informationen finden Sie unter Konten mithilfe von Automatisierung bereitstellen und aktualisieren.

Vermeiden Sie eine gemischte Steuerung bei der Konfiguration von Regionen

Es ist wichtig, alle Konten in einer OU zu aktualisieren, nachdem Sie die AWS Control Tower Governance auf eine neue AWS-Region erweitert haben und nachdem Sie die AWS Control Tower Governance aus einer Region entfernt haben.

Eine gemischte Verwaltung ist eine unerwünschte Situation, die auftreten kann, wenn die Kontrollen, die eine OU regeln, nicht vollständig mit den Kontrollen übereinstimmen, die die einzelnen Konten innerhalb einer OU regeln. In einer Organisationseinheit kommt es zu einer gemischten Verwaltung, wenn die Konten nicht aktualisiert werden, nachdem der AWS Control Tower die Governance auf eine neue AWS-Region erweitert oder die Governance aufgehoben hat.

In dieser Situation können für bestimmte Konten innerhalb einer OU in verschiedenen Regionen unterschiedliche Kontrollen gelten, verglichen mit anderen Konten in der OU oder im Vergleich zur allgemeinen Governance-Position der Landezone.

Wenn Sie in einer Organisationseinheit mit gemischter Verwaltung ein neues Konto bereitstellen, erhält dieses neue Konto dieselbe (aktualisierte) Regions- und Organisationsstruktur wie die Landezone. Bestehende Konten, die noch nicht aktualisiert wurden, erhalten jedoch nicht den aktualisierten Verwaltungsstatus der Region.

Im Allgemeinen kann eine gemischte Verwaltung zu widersprüchlichen oder ungenauen Statusindikatoren in der AWS Control Tower-Konsole führen. Beispielsweise werden bei gemischter Verwaltung Opt-in-Regionen in registrierten Organisationseinheiten für Konten, die noch nicht aktualisiert wurden, mit dem Status Nicht verwaltet angezeigt.

> **Note**
>
> Im AWS Control Tower ist es nicht möglich, Kontrollen in einem Zustand mit gemischter Verwaltung zu aktivieren.

Verhalten der Kontrollen bei gemischter Steuerung

- Bei gemischter Verwaltung kann AWS Control Tower Kontrollen, die auf AWS Config Regeln (d. h. detektivischen Kontrollen) basieren, in Regionen, die in der Organisationseinheit bereits als verwaltet angezeigt werden, nicht konsistent bereitstellen, da einige Konten

in der Organisationseinheit nicht aktualisiert wurden. Möglicherweise erhalten Sie eine `FAILED_TO_ENABLE` Fehlermeldung.

- Wenn Sie bei gemischter Verwaltung die Verwaltung der Landezone auf eine Opt-in-Region ausdehnen, während noch kein Konto in der OU aktualisiert wurde, schlägt der `EnableControl` API-Vorgang auf der OU fehl, um detektivische und proaktive Kontrollen durchzuführen. Sie erhalten eine `FAILED_TO_ENABLE` Fehlermeldung, da nicht aktualisierte Mitgliedskonten innerhalb der OU noch nicht für diese Regionen angemeldet wurden.
- Bei gemischter Verwaltung: Kontrollen, die Teil des Security Hub Service-managed CSPM-Standards sind: Der AWS Control Tower kann die Einhaltung von Vorschriften in Regionen, in denen eine Diskrepanz zwischen der Konfiguration der Landezone und den Konten besteht, die nicht aktualisiert werden, nicht korrekt melden.
- Eine gemischte Steuerung ändert nichts am Verhalten der SCP-based Kontrollen (präventive Kontrollen), die einheitlich für jedes Konto in einer OU in jeder regulierten Region gelten.

> **Note**
>
> Gemischte Regierungsführung ist nicht gleichbedeutend mit Drift, und sie wird auch nicht als Drift gemeldet.

Um eine gemischte Regierungsführung zu reparieren

- Kunden sind jetzt in der Lage, gemischte Verwaltungsstrukturen zu reparieren, indem sie die regionalen Kontrollen neu einrichten. Alle nicht globalen Kontrollen sind regional (detektivische und proaktive Kontrollen). Sie werden durch ein Warnbanner darauf hingewiesen, dass Ihre Organisationseinheit einer gemischten Unternehmensstruktur unterliegt.

Überlegungen zur Aktivierung AWS Opt-in-Regionen

Obwohl die meisten Regionen standardmäßig für Sie aktiv AWS-Regionen sind AWS-Konto, werden bestimmte Regionen nur aktiviert, wenn Sie sie manuell auswählen. In diesem Dokument werden diese Regionen als Opt-in-Regionen bezeichnet. Im Gegensatz dazu werden Regionen, die standardmäßig aktiv sind, sobald Ihre AWS-Konto erstellt wurde, als kommerzielle Regionen, Standardregionen oder einfach als Regionen bezeichnet.

Der Begriff Opt-In hat eine historische Grundlage. Alle Regionen, die nach dem 20. März 2019 AWS-Regionen eingeführt wurden, werden als Opt-In-Regionen bereitgestellt. In einer Region, in der Sie sich anmelden, ist Ihr Konto in dieser Region nicht aktiviert — und Ihre Identität wird nicht auf die Region übertragen — es sei denn, Sie entscheiden sich für die Nutzung dieser Region. Alle Daten, die über den IAM-Dienst verwaltet werden, gelten als Identitätsdaten, einschließlich Benutzer, Gruppen, Rollen, Richtlinien, Identitätsanbieter, die zugehörigen Daten (z. B. X.509 Signaturzertifikate oder kontextspezifische Anmeldeinformationen) und andere Einstellungen auf Kontoebene, wie die Kennwortrichtlinie und der Kontoalias.

Sie können Opt-in-Regionen bei der Einrichtung der Landing Zone automatisch aktivieren, indem Sie sie auswählen. Deine Landezone wird in allen ausgewählten Regionen aktiv.

Wenn Sie eine Opt-in-Region als Ihre AWS Control Tower-Heimatregion auswählen, aktivieren Sie diese zunächst, indem Sie die Schritte unter Region aktivieren befolgen, wenn Sie an der AWS Management Console angemeldet sind. Um Ihre eigenen bestehenden Log-Archiv- und Audit-Konten aus einer Opt-in-Region mitzubringen, aktivieren Sie diese Region zuerst manuell.

Die AWS Opt-in-Regionen umfassen mehrere Regionen, in denen AWS Control Tower verfügbar ist:

- Region Asien-Pazifik (Hongkong), AP-East-1
- Region Asien-Pazifik (Jakarta), ap-southeast-3
- Region Europa (Mailand), EU-Süd-1
- Region Afrika (Kapstadt), af-south-1
- Region Naher Osten (Bahrain), mich-süd-1
- Israel (Tel Aviv), Zentral-1
- Region Naher Osten (VAE), me-central-1
- Region Europa (Spanien), EU-Süd-2
- Region Asien-Pazifik (Hyderabad), AP-Süd-2
- Region Europa (Zürich), eu-central-2
- Region Asien-Pazifik (Melbourne), AP-Southeast-4
- Region Kanada West (Calgary), ca-west-1
- Asien-Pazifik (Thailand), ap-southeast-7
- Mexiko (Zentral), mx-central-1
- Asien-Pazifik (Taipeh), AP-East-2
- Asien-Pazifik (Neuseeland), ap-southeast-6

AWS Control Tower verfügt über einige Steuerelemente, die in den Opt-in-Regionen anders funktionieren als in den Standardregionen (andere kommerzielle Regionen). Weitere Informationen finden Sie unter Einschränkungen bei der Steuerung. Im Folgenden finden Sie einige Überlegungen, die Sie bei der Bereitstellung von Workloads in Opt-in-Regionen berücksichtigen sollten.

> **Steuern oder aktivieren?**
>
> Denken Sie daran, dass das Regieren einer Region eine Aktion ist, die Sie in der AWS Control Tower-Konsole auswählen können, sodass die Kontrollen in der Region angewendet werden können. Die Aktivierung oder Deaktivierung einer Opt-in-Region ist eine andere Aktion, die Sie in der AWS Konsole auswählen können. Dadurch wird die Region für Ihr Konto geöffnet, sodass Sie Ressourcen und Workloads in der Region bereitstellen können.

Überlegungen in Bezug auf das Verhalten

- Wenn du dich für die Verwaltung deiner Opt-in-Regionen entscheidest, empfehlen wir dir, keine deiner regulierten Opt-in-Regionen zu deaktivieren (dich abzumelden), da dies zum Ausfall deiner Workloads führen kann. Der AWS Control Tower erlaubt keine Deaktivierung einer regulierten Region von der AWS Control Tower-Konsole aus. Achten Sie jedoch darauf, dass Sie die regulierten Regionen nicht von einer Quelle außerhalb des AWS Control Tower aus deaktivieren, z. B. über die AWS Rechnungskonsole oder das SDK. AWS
- Wenn der AWS Control Tower die Verwaltung auf eine Opt-in-Region ausdehnt, wird die Region in allen Mitgliedskonten aktiviert (Opt-In). Wenn Sie eine Region aus der Governance entfernen, deaktiviert AWS Control Tower die Region nicht in den Mitgliedskonten (Opt-Out).
- Bei der Abwahl einer Region überspringt AWS Control Tower das Entfernen von Ressourcen aus einer Opt-in-Region, wenn diese Region manuell für ein Konto aus einer Quelle außerhalb des AWS Control Tower deaktiviert wurde, wie z. B. die AWS Rechnungskonsole oder das SDK. AWS Wir empfehlen, Ressourcen aus den Regionen zu entfernen, die Sie deaktiviert haben. Andernfalls können Ihnen unerwartete Abrechnungsgebühren für diese Ressourcen berechnet werden.
- Wenn Ihre Landezone außer Betrieb genommen wird, bereinigt der AWS Control Tower die Ressourcen in allen regierten Regionen, einschließlich der Opt-in-Regionen. Der AWS Control Tower deaktiviert die Opt-in-Regionen jedoch nicht. Sie können die Opt-in-Regionen als zusätzlichen Schritt nach der Außerbetriebnahme deaktivieren.
- Wenn Ihre Heimatregion eine Opt-in-Region ist und Sie beabsichtigen, bestehende Konten als Log-Archiv- und Audit-Konten zu registrieren, müssen Sie die Opt-in-Region manuell aktivieren, bevor Sie sie als Heimatregion für Ihre Landezone auswählen können. Siehe Eine Region aktivieren.

- Wenn AWS Control Tower mit einer Opt-in-Region als Ihrer Heimatregion eingerichtet ist und Sie den AWS Control Tower-Service von der AWS Konsole aus in einer anderen Region aufrufen, leitet Sie die Konsole nicht automatisch in die Heimatregion weiter.
- Die zugrunde liegende API hat Kapazitätsgrenzen, wodurch sich die Latenz je nach Anzahl der Regionen, Konten und Servicelast von einigen Minuten auf viele Stunden erhöhen kann. Es hat sich bewährt, sich nur für diejenigen anzumelden, AWS-Regionen in denen Sie Workloads ausführen werden, und melden Sie sich jeweils für eine Region an.

Wichtige Einschränkungen für Unternehmensführung und Konten

- Wenn 16 oder mehr kommerzielle Regionen, in denen der AWS Control Tower verfügbar ist, reguliert werden, einschließlich Opt-in-Regionen, wird die Obergrenze für die Anzahl der Konten pro Organisationseinheit (OU) bei der Registrierung einer OU reduziert. Weitere Informationen finden Sie unter Einschränkungen, die auf den zugrunde liegenden AWS Diensten basieren.

Konfigurieren Sie die Region Deny Control

AWS Control Tower bietet zwei Kontrollen zum Verweigern von Regionen. Ein Steuerelement gilt`AWS-GR_REGION_DENY`, wenn es aktiviert ist, für die gesamte Landezone. Ein anderes Steuerelement kann`CT.MULTISERVICE.PV.1`, wenn es aktiviert ist, für bestimmte Organisationseinheiten gelten, die Sie angeben. Weitere Informationen finden Sie unter Zugriff verweigern auf der AWS Grundlage der angeforderten AWS-Region und regionalen Verweigerungskontrolle, die auf die Organisationseinheit angewendet wurde.

Überlegungen zur Region verweigert die Kontrolle über die Landezone

Die Region, die die Kontrolle verweigert, `AWS-GR_REGION_DENY` ist einzigartig, da sie für die gesamte Landezone gilt und nicht für eine bestimmte OU. Um die Region Deny Control zu konfigurieren, gehen Sie zur Seite mit den Landing Zone-Einstellungen und wählen Sie Einstellungen ändern aus.

- Diese Einstellung kann zu einem späteren Zeitpunkt geändert werden.
- Wenn diese Option aktiviert ist, gilt diese Steuerung für alle Organisationseinheiten, in denen die `AWSControlTowerBaseline` Option aktiviert ist.
- Dieses Steuerelement kann nicht für einzelne Organisationseinheiten konfiguriert werden.

> **Note**
>
> Bevor Sie die Steuerung „Region verweigern“ aktivieren, stellen Sie sicher, dass in diesen Regionen keine Ressourcen vorhanden sind, da Sie nach dem Anwenden der Steuerung keinen Zugriff mehr auf Ihre Ressourcen haben. Solange die Steuerung aktiviert ist, können Sie in den verbotenen Regionen keine Ressourcen bereitstellen.

Wenn Sie das Steuerelement aktivieren, gilt es für alle Organisationseinheiten der obersten Ebene, in denen das Steuerelement `AWSControlTowerBaseline` aktiviert ist, und es wird an Organisationseinheiten vererbt, die sich weiter unten in der Organisationshierarchie befinden. Wenn Sie die Kontrolle entfernen, wird sie für alle zuvor angewendeten Organisationseinheiten entfernt. Alle nicht regulierten Regionen im AWS Control Tower bleiben im Status Nicht verwaltet, und Sie können Ressourcen in Regionen außerhalb der Verfügbarkeit von AWS Control Tower bereitstellen.

> **Ausnahmen**
>
> Sie können den Zugriff auf Ihre Heimatregion nicht verweigern. Bestimmte globale AWS Dienste wie IAM und AWS Organizations sind von der Region Deny Control ausgenommen. Weitere Informationen finden Sie unter Zugriff auf AWS je nach Anforderung verweigern. AWS-Region

- Vollständiger Kontrollname: Verweigert den Zugriff auf AWS basierend auf der angeforderten AWS Region für die Landezone
- Beschreibung der Steuerung: Verbietet den Zugriff auf nicht aufgeführte Operationen in globalen und regionalen Diensten außerhalb der für die Landezone angegebenen Regionen.
- Es handelt sich um eine elektive Kontrolle mit präventiver Anleitung.

Die Vorlage für den SCP Region Deny Control finden Sie unter Zugriff verweigern auf der AWS Grundlage der AWS-Region in der AWS Control Tower Control-Referenz angeforderten Informationen. Der AWS Control Tower SCP ist dem SCP für ähnlich AWS Organizations, aber nicht identisch.

Sie können regionale Service-Endpunkte auf der Seite Regionale Services ermitteln.

Überlegungen zur OU-level Region verweigern die Kontrolle

Die wichtigste Überlegung, ob die OU-level Region die Kontrolle verweigert, ist die Frage, wie sie mit der Landezone interagiert. Die Region verweigert die Kontrolle, wenn beide aktiviert sind. Weitere Informationen finden Sie unter Auf die OU angewendete Region-Deny-Control.

Vielleicht möchten Sie auch den Artikel Regionsverweigerungskontrolle konfigurieren lesen.

Informationen AWS-Konten im AWS Control Tower

An AWS-Konto ist der Container für all Ihre eigenen Ressourcen. Zu diesen Ressourcen gehören die vom Konto akzeptierten AWS Identity and Access Management (IAM-) Identitäten, die bestimmen, wer Zugriff auf dieses Konto hat. IAM-Identitäten können Benutzer, Gruppen, Rollen und mehr umfassen. Weitere Informationen zur Arbeit mit IAM, Benutzern, Rollen und Richtlinien in AWS Control Tower finden Sie unter Identitäts- und Zugriffsmanagement in AWS Control Tower.

Ressourcen und Zeit für die Kontoerstellung

Wenn AWS Control Tower ein Konto erstellt oder registriert, stellt es die mindestens erforderliche Ressourcenkonfiguration für das Konto bereit. Es kann beispielsweise Ressourcen in Form von Account Factory Factory-Vorlagen und andere Ressourcen in Ihrer landing zone enthalten, wie IAM-Rollen, AWS CloudTrail Trails, von Service Catalog bereitgestellte Produkte und IAM Identity Center-Benutzer. AWS Control Tower stellt gemäß der Kontrollkonfiguration auch Ressourcen für die Organisationseinheit (OU) bereit, in der das neue Konto ein Mitgliedskonto werden soll.

AWS Control Tower orchestriert die Bereitstellung dieser Ressourcen in Ihrem Namen. Es kann mehrere Minuten pro Ressource dauern, bis die Bereitstellung abgeschlossen ist. Berücksichtigen Sie daher die Gesamtzeit, bevor Sie ein Konto erstellen oder registrieren. Weitere Informationen zur Verwaltung von Ressourcen in Ihren Konten finden Sie unterAnleitung zur Erstellung und Änderung von AWS Control Tower Tower-Ressourcen.

Was passiert, wenn AWS Control Tower ein Konto erstellt

Neue Konten in AWS Control Tower werden durch eine Interaktion zwischen AWS Control Tower AWS Organizations, und erstellt und AWS Service Catalog dann bereitgestellt. Sie können über die AWS Control Tower Tower-Konsole Konten erstellen und bestehende Konten registrieren. Ausführliche Schritte zur Registrierung eines vorhandenen AWS-Konto über die AWS Control Tower Tower-Konsole finden Sie unterRegistrieren Sie ein vorhandenes Konto über die AWS Control Tower-Konsole.

Hinter den Kulissen der Kontoerstellung

1. Sie initiieren die Anfrage beispielsweise von der AWS Control Tower Account Factory Factory-Seite oder direkt von der AWS Service Catalog Konsole aus oder indem Sie die Service `ProvisionProduct` Catalog-API aufrufen.

2. AWS Service Catalog ruft AWS Control Tower auf.
3. AWS Control Tower startet einen Workflow, der in einem ersten Schritt die AWS Organizations `CreateAccount` API aufruft.
4. Nach der AWS Organizations Erstellung des Kontos schließt AWS Control Tower den Bereitstellungsprozess ab, indem er Blueprints und Kontrollen anwendet.
5. Service Catalog fragt weiterhin AWS Control Tower ab, um zu überprüfen, ob der Bereitstellungsprozess abgeschlossen ist.
6. Wenn der Workflow in AWS Control Tower abgeschlossen ist, stellt Service Catalog den Status des Kontos fest und informiert Sie (den Anforderer) über das Ergebnis.

Überlegungen zur Verwendung vorhandener Sicherheits- oder Protokollkonten

Bevor ein Konto AWS-Konto als Sicherheit (Standardname: Config Aggregator) oder als Protokollierung (Standardname: CloudTrail Administrator) akzeptiert wird, überprüft AWS Control Tower das Konto auf Ressourcen, die mit den AWS Control Tower Tower-Anforderungen in Konflikt stehen. Beispielsweise haben Sie möglicherweise einen Logging-Bucket mit demselben Namen, den AWS Control Tower benötigt. Außerdem überprüft AWS Control Tower, ob das Konto Ressourcen bereitstellen kann, indem beispielsweise sichergestellt wird, dass AWS -Security-Token-Service (AWS STS) aktiviert ist, dass das Konto nicht gesperrt ist und dass AWS Control Tower berechtigt ist, Ressourcen innerhalb des Kontos bereitzustellen.

AWS Control Tower entfernt keine vorhandenen Ressourcen in den von Ihnen bereitgestellten Protokollierungs- und Sicherheitskonten. Wenn Sie es jedoch aktivieren, verhindert die Deny Control Control in der AWS-Control-Tower-Region den Zugriff auf Ressourcen in verweigerten Regionen.

> **Sicherheit für Ihre Konten**
>
> In der AWS Organizations Dokumentation finden Sie Hinweise zu bewährten Methoden zum Schutz der Sicherheit Ihres AWS Control Tower Tower-Verwaltungskontos und Ihrer Mitgliedskonten.
>
> - Bewährte Methoden für das Verwaltungskonto
> - Bewährte Methoden für Mitgliedskonten

Konten zur Serviceintegration

AWS Control Tower verwendet drei spezielle Konten AWS-Konten: das Verwaltungskonto, das Config-Aggregator-Konto und das CloudTrailAdministratorkonto. AWS Control Tower bezeichnet das Config-Aggregator-Konto und das CloudTrail Administratorkonto als Service-Integrationskonten.

> **Ältere Kontonamen**
>
> In landing zone Zone-Versionen vor 4.0 wurden diese Konten als gemeinsame Konten (oder manchmal als Kernkonten) bezeichnet.

- Sie können benutzerdefinierte Namen für die Serviceintegrationskonten auswählen, wenn Sie Ihre landing zone einrichten. Informationen zum Ändern eines Kontonamens finden Sie unter Externes Ändern von AWS Control Tower Tower-Ressourcennamen.
- Sie können bei der ersten Einrichtung der landing zone AWS-Konto auch ein vorhandenes AWS-Control-Tower-Serviceintegrationskonto angeben. Diese Option macht es überflüssig, dass AWS Control Tower neue Konten erstellt. (Dies ist eine einmalige Auswahl.)

Weitere Informationen zu den Serviceintegrationskonten und den zugehörigen Ressourcen finden Sie unterRessourcen, die in den Serviceintegrationskonten erstellt wurden.

Verwaltungskonto

Dadurch AWS-Konto wird AWS Control Tower gestartet. Standardmäßig haben der Root-Benutzer für dieses Konto und der IAM-Benutzer oder der IAM-Administratorbenutzer für dieses Konto vollen Zugriff auf alle Ressourcen in Ihrer landing zone.

> **Note**
>
> Als bewährte Methode empfehlen wir, sich als IAM Identity Center-Benutzer mit Administratorrechten anzumelden, wenn Sie administrative Funktionen in der AWS Control Tower Tower-Konsole ausführen, anstatt sich als Root-Benutzer oder IAM-Administrator-Benutzer für dieses Konto anzumelden.

Weitere Informationen zu den Rollen und Ressourcen, die im Verwaltungskonto verfügbar sind, finden Sie unter. Ressourcen, die in den Serviceintegrationskonten erstellt wurden

CloudTrail Administratorkonto

AWS Control Tower richtet das CloudTrail Administratorkonto ein, wenn Sie die AWS CloudTrail zentrale Protokollierungsintegration aktivieren. Alternativ können Sie ein vorhandenes AWS Konto als CloudTrail Administratorkonto verwenden. Möglicherweise kennen Sie dieses Konto unter seinem früheren Namen: dem Protokollarchivkonto.

Dieses Konto enthält einen zentralen Amazon S3 S3-Bucket, der Protokolldateien für alle anderen Konten in Ihrer landing zone speichert. In landing zone Zone-Versionen vor 4.0 speichert dieser Bucket AWS CloudTrail sowohl AWS Config Protokolldateien als auch Protokolldateien. In landing zone Version 4.0 und höher speichert dieser Bucket nur AWS CloudTrail Protokolldateien. AWS Config speichert seine Protokolldateien in einem speziellen Bucket im Config-Aggregator-Konto.

Es hat sich bewährt, den Zugriff auf dieses Konto auf Teams zu beschränken, die für Compliance und Untersuchungen verantwortlich sind, sowie auf die entsprechenden Sicherheits- oder Audit-Tools. Sie können dieses Konto für automatisierte Sicherheitsaudits verwenden. Sie können auch benutzerdefinierte AWS-Config-Regeln Funktionen wie Lambda-Funktionen hosten, um Behebungsmaßnahmen durchzuführen.

> **Amazon S3 S3-Bucket-Richtlinie**
>
> Für AWS Control Tower landing zone Version 3.3 und höher müssen Konten eine `aws:SourceOrgID` Bedingung für Schreibberechtigungen für Ihren Audit-Bucket erfüllen. Diese Bedingung stellt sicher, dass CloudTrail nur Protokolle im Namen von Konten innerhalb Ihrer Organisation in Ihren S3-Bucket geschrieben werden können. Dadurch wird verhindert, dass CloudTrail Protokolle außerhalb Ihrer Organisation in Ihren AWS Control Tower S3-Bucket schreiben. Weitere Informationen finden Sie unter AWS Control Tower-Landingzone, Version 3.3.

Weitere Informationen zu den Rollen und Ressourcen, die im Protokollarchiv-Konto verfügbar sind, finden Sie unter CloudTrail Ressourcen für Administratorkonten

> **Note**
>
> Diese Protokolle können nicht geändert werden. Alle Protokolle werden für Prüfungs- und Compliance-Untersuchungen im Zusammenhang mit Kontoaktivitäten gespeichert.

Aggregatorkonto konfigurieren

AWS Control Tower richtet das Config-Aggregator-Konto ein, wenn Sie die AWS Config Service-Integration aktivieren. Alternativ können Sie ein vorhandenes AWS Konto als Config-Aggregator-Konto verwenden. Möglicherweise kennen Sie dieses Konto unter seinem früheren Namen: dem Auditkonto.

Das Config-Aggregator-Konto sollte auf Sicherheits- und Compliance-Teams mit kontoübergreifenden Rollen als Auditor (schreibgeschützt) und Administrator (voller Zugriff) für alle Konten in der landing zone beschränkt sein. Diese Rollen sollen von Sicherheits- und Compliance-Teams für folgende Zwecke verwendet werden:

- Führen Sie Audits mithilfe von AWS Mechanismen durch, z. B. durch das Hosten von Lambda-Funktionen für benutzerdefinierte AWS Config Regeln.
- Führen Sie automatisierte Sicherheitsoperationen durch, z. B. Abhilfemaßnahmen.

Das Config-Aggregator-Konto erhält auch Benachrichtigungen über den Amazon Simple Notification Service (Amazon SNS) -Service. Sie können drei Kategorien von Benachrichtigungen erhalten:

- Alle Konfigurationsereignisse — In diesem Thema werden alle CloudTrail AWS Config Benachrichtigungen von allen Konten in Ihrer landing zone zusammengefasst.
- Aggregierte Sicherheitsbenachrichtigungen — In diesem Thema werden alle Sicherheitsbenachrichtigungen zu bestimmten CloudWatch Ereignissen, Ereignissen zur Änderung des AWS-Config-Regeln Compliance-Status und GuardDuty zu Ergebnissen zusammengefasst.
- Drift-Benachrichtigungen — In diesem Thema werden alle Drift-Warnungen zusammengefasst, die für alle Konten, Benutzer, OUs und SCPs in Ihrer landing zone entdeckt wurden. Weitere Informationen zur Drift finden Sie unter Abweichungen im AWS Control Tower erkennen und beheben.

Audit-Benachrichtigungen, die innerhalb eines Mitgliedskontos ausgelöst werden, können auch Benachrichtigungen an ein lokales Amazon SNS SNS-Thema senden. Diese Funktion ermöglicht es Kontoadministratoren, Audit-Benachrichtigungen zu abonnieren, die für ein einzelnes Mitgliedskonto spezifisch sind. Dadurch können Administratoren Probleme lösen, die ein einzelnes Konto betreffen, und gleichzeitig alle Kontobenachrichtigungen in Ihrem zentralen Config-Aggregator-Konto zusammenfassen. Weitere Informationen finden Sie im Amazon Simple Notification Service-Entwicklerhandbuch.

Weitere Informationen zu den Rollen und Ressourcen, die im Config-Aggregator-Konto verfügbar sind, finden Sie unterRessourcen für Config-Aggregatorkonten.

Weitere Informationen zur programmatischen Prüfung finden Sie unter Programmatische Rollen und Vertrauensbeziehungen für das AWS Control Tower Tower-Auditkonto.

> **Important**
>
> Die E-Mail-Adresse, die Sie für das Config-Aggregator-Konto angeben, erhält E-Mails mit AWS Benachrichtigungen und Abonnementbestätigungen von allen, die von AWS Control Tower AWS-Region unterstützt werden. Um Compliance-E-Mails in Ihrem Config-Aggregator-Konto zu erhalten, müssen Sie in jeder E-Mail, die von AWS Control Tower AWS-Region unterstützt wird, den Link Abonnement bestätigen auswählen.

Ressourcen, die in den Serviceintegrationskonten erstellt wurden

In diesem Abschnitt werden die Ressourcen angezeigt, die AWS Control Tower in den Service-Integrationskonten erstellt, wenn Sie Ihre landing zone einrichten.

Informationen zu Ressourcen für Mitgliedskonten finden Sie unterÜberlegungen zu Ressourcen für Account Factory.

Ressourcen für Verwaltungskonten

Wenn Sie Ihre landing zone einrichten, werden die folgenden AWS Ressourcen in Ihrem Verwaltungskonto erstellt.

AWS Service	Ressourcentyp	Ressourcenname
AWS Organizations	Konten	Config aggregator (audit) CloudTrail administrator (log archive)
AWS Organizations	Organisationseinheiten	Security Sandbox
AWS Organizations	Service-Kontrollrichtlinien	aws-guardrails-*

AWS Service	Ressourcentyp	Ressourcenname
AWS CloudFormation	Stacks	AWSControlTowerBP-BASELINE-CLOUDTRAIL-MASTER AWSControlTowerBP-BASELINE-CONFIG-MASTER(in landing zone Version 2.6 und höher; nicht bereitgestellt in landing zone Version 4.0 und höher)

AWS Service	Ressourcentyp	Ressourcenname
AWS CloudFormation	StackSets	AWSControlTowerBP-BASELINE-CLOUDTRAIL(Nicht in landing zone Version 3.0 und höher bereitgestellt) AWSControlTowerBP-BASELINE-CLOUDWATCH AWSControlTowerBP-BASELINE-CONFIG AWSControlTowerBP-BASELINE-ROLES AWSControlTowerBP-BASELINE-SERVICE-ROLES AWSControlTowerBP-BASELINE-SERVICE-LINKED-ROLE(Wird in landing zone Version 3.2 und höher eingesetzt) AWSControlTowerBP-SECURITY-TOPICS AWSControlTowerLoggingResources AWSControlTowerSecurityResources AWSControlTowerExecutionRole AWSControlTowerBP-CONFIG-CENTRAL-S3-

AWS Service	Ressourcentyp	Ressourcenname
		BUCKET(Wird in landing zone Version 4.0 und höher eingesetzt)
AWS Service Catalog	Produkt	AWS Control Tower Account Factory
AWS Config	Aggregator	aws-controltower-ConfigAggregatorForOrganizations(Nicht in landing zone Version 4.0 und höher bereitgestellt)
AWS CloudTrail	Trail	aws-controltower-BaselineCloudTrail
Amazon CloudWatch	CloudWatch Logs	aws-controltower/CloudTrail Logs
AWS Identity and Access Management	Rollen	AWSControlTowerAdmin AWSControlTowerStackSetRole AWSControlTowerCloudTrailRolePolicy
AWS Identity and Access Management	Richtlinien	AWSControlTowerServiceRolePolicy AWSControlTowerAdminPolicy AWSControlTowerCloudTrailRolePolicy AWSControlTowerStackSetRolePolicy

AWS Service	Ressourcentyp	Ressourcenname
AWS IAM Identity Center	Verzeichnisgruppen	AWSAccountFactory AWSAuditAccountAdmins AWSControlTowerAdmins AWSLogArchiveAdmins AWSLogArchiveViewers AWSSecurityAuditors AWSSecurityAuditPowerUsers AWSServiceCatalogAdmins
AWS IAM Identity Center	Berechtigungssätze	AWSAdministratorAccess AWSPowerUserAccess AWSServiceCatalogAdminFullAccess AWSServiceCatalogEndUserAccess AWSReadOnlyAccess AWSOrganizationsFullAccess

Note

Das CloudFormation StackSet `BP_BASELINE_CLOUDTRAIL` wird in landing zone Zone-Versionen 3.0 oder höher nicht bereitgestellt. In früheren Versionen der landing zone ist sie jedoch weiterhin vorhanden, bis Sie Ihre landing zone aktualisieren.
Ab Juni 2025 setzt AWS Control Tower Detective Controls als serviceverknüpfte AWS Config Regeln direkt in registrierten Konten ein, statt sie über. CloudFormation StackSets Die StackSets `AWSControlTowerGuardrailAWS-GR-AUDIT-BUCKET-PUBLIC-READ-`

`PROHIBITED` und `AWSControlTowerGuardrailAWS-GR-AUDIT-BUCKET-PUBLIC-WRITE-PROHIBITED` und die zugehörigen Stack-Instances werden nicht mehr bereitgestellt. Weitere Informationen finden Sie unter Support für Detective Controls, die als servicebasierte AWS Config-Regeln bereitgestellt werden.

CloudTrail Ressourcen für Administratorkonten

Wenn Sie Ihre landing zone einrichten, werden die folgenden AWS Ressourcen in Ihrem CloudTrail Administratorkonto erstellt.

AWS Service	Ressourcentyp	Ressourcenname
AWS CloudFormation	Stacks	StackSet-AWSControlTowerBP-BASELINE-CLOUDWATCH- StackSet-AWSControlTowerBP-BASELINE-CONFIG- StackSet-AWSControlTowerBP-BASELINE-CLOUDTRAIL- StackSet-AWSControlTowerBP-BASELINE-SERVICE-ROLES- StackSet-AWSControlTowerBP-BASELINE-SERVICE-LINKED-ROLE-(In landing zone version 3.2 and later) StackSet-AWSControlTowerBP-BASELINE-ROLES-

AWS Service	Ressourcentyp	Ressourcenname
		StackSet-AWSContro lTowerLoggingResources-
AWS Config	AWS-Config-Regeln	AWSControlTower_AW S-GR_AUDIT_BUCKET_ PUBLIC_READ_PROHIBITED AWSControlTower_AW S-GR_AUDIT_BUCKET_ PUBLIC_WRITE_PROHI BITED
AWS CloudTrail	Trails	aws-controltower-BaselineCl oudTrail
Amazon CloudWatch	CloudWatch Regeln für Veranstaltungen	aws-controltower-ConfigComp lianceChangeEventRule
Amazon CloudWatch	CloudWatch Logs	/aws/lambda/aws-controltowe r-NotificationForwarder

AWS Service	Ressourcentyp	Ressourcenname
AWS Identity and Access Management	Rollen	aws-controltower-AdministratorExecutionRole aws-controltower-CloudWatchLogsRole aws-controltower-ConfigRecorderRole aws-controltower-ForwardSnsNotificationRole aws-controltower-ReadOnlyExecutionRole AWSControlTowerExecution AWSServiceRoleForAWSControlTower
AWS Identity and Access Management	Richtlinien	AWSControlTowerServiceRolePolicy
Amazon Simple Notification Service	Topics	aws-controltower-SecurityNotifications
AWS Lambda	Anwendungen	StackSet-AWSControlTowerBP-BASELINE-CLOUDWATCH-*
AWS Lambda	Funktionen	aws-controltower-NotificationForwarder
Amazon Simple Storage Service	Buckets	aws-controltower-logs-* aws-controltower-s3-access-logs-*

Ressourcen für Config-Aggregatorkonten

Wenn Sie Ihre landing zone einrichten, werden die folgenden AWS Ressourcen in Ihrem Config-Aggregator-Konto erstellt.

AWS Service	Ressourcentyp	Ressourcenname
AWS CloudFormation	Stacks	StackSet-AWSControlTowerBP-BASELINE-CLOUDWATCH- StackSet-AWSControlTowerBP-BASELINE-CONFIG- StackSet-AWSControlTowerBP-BASELINE-CLOUDTRAIL- StackSet-AWSControlTowerBP-BASELINE-SERVICE-ROLES- StackSet-AWSControlTowerBP-BASELINE-SERVICE-LINKED-ROLE-(In landing zone version 3.2 and later) StackSet-AWSControlTowerBP-SECURITY-TOPICS- StackSet-AWSControlTowerBP-BASELINE-ROLES- StackSet-AWSControlTowerSecurityResources-*

AWS Service	Ressourcentyp	Ressourcenname
		StackSet-AWSControlTowerBP-CONFIG-CENTRAL-S3-BUCKET-(Wird in landing zone Version 4.0 und höher eingesetzt)
AWS Config	Aggregator	aws-controltower-GuardrailsComplianceAggregator(Nicht in landing zone Version 4.0 und höher bereitgestellt)
AWS Config	Aggregator	aws-controltower-ConfigAggregatorForOrganizations(Wird in landing zone Version 4.0 und höher eingesetzt)
AWS Config	AWS-Config-Regeln	AWSControlTower_AWS-GR_AUDIT_BUCKET_PUBLIC_READ_PROHIBITED AWSControlTower_AWS-GR_AUDIT_BUCKET_PUBLIC_WRITE_PROHIBITED
AWS CloudTrail	Trail	aws-controltower-BaselineCloudTrail
Amazon CloudWatch	CloudWatch Regeln für Veranstaltungen	aws-controltower-ConfigComplianceChangeEventRule
Amazon CloudWatch	CloudWatch Logs	/aws/lambda/aws-controltower-NotificationForwarder

AWS Service	Ressourcentyp	Ressourcenname
AWS Identity and Access Management	Rollen	aws-controltower-AdministratorExecutionRole aws-controltower-CloudWatchLogsRole aws-controltower-ConfigRecorderRole aws-controltower-ForwardSnsNotificationRole aws-controltower-ReadOnlyExecutionRole aws-controltower-AuditAdministratorRole aws-controltower-AuditReadOnlyRole AWSControlTowerExecution AWSServiceRoleForAWSControlTower
AWS Identity and Access Management	Richtlinien	AWSControlTowerServiceRolePolicy
Amazon Simple Notification Service	Topics	aws-controltower-AggregateSecurityNotifications aws-controltower-AllConfigNotifications aws-controltower-SecurityNotifications

AWS Service	Ressourcentyp	Ressourcenname
AWS Lambda	Funktionen	aws-controltower-NotificationForwarder
Amazon Simple Storage Service	Buckets	aws-controltower-config-logs-*(Wird in landing zone Version 4.0 und höher eingesetzt) aws-controltower-config-access-logs-*(Wird in landing zone Version 4.0 und höher eingesetzt)

Über Mitgliedskonten

Mitgliedskonten sind die Konten, über die Ihre Benutzer ihre AWS Workloads ausführen. AWS Control Tower Tower-Mitgliedskonten können mit verschiedenen Methoden, einschließlich automatisierter Methoden, erstellt und angepasst werden. In einigen Fällen können Sie bestehende Daten AWS-Konten in AWS Control Tower übernehmen. Wenn Mitgliedskonten erstellt oder registriert werden, müssen sie innerhalb einer Organisationseinheit (OU) existieren, die in der AWS Control Tower-Konsole erstellt oder bei AWS Control Tower registriert wurde. Weitere Informationen finden Sie in diesen verwandten Themen:

- Methoden der Bereitstellung
- Bereitstellung und Verwaltung von Konten mit Account Factory
- Automatisieren Sie Aufgaben im AWS Control Tower
- Konten mit automatischer Registrierung verschieben und registrieren
- Bereitstellung von Konten mit AWS Control Tower Account Factory für Terraform (AFT)
- AWS Terminologie und Konzepte für Organizations im AWS Organizations Benutzerhandbuch.

> **Konten und Kontrollen**
>
> Mitgliedskonten können bei AWS Control Tower registriert oder deren Registrierung aufgehoben werden. Die Kontrollen gelten für registrierte und nicht registrierte Konten

unterschiedlich, und für Konten in verschachtelten Organisationseinheiten können die Kontrollen aufgrund der Vererbung gelten.

Informationen zu Ressourcen für Mitgliedskonten, die AWS Control Tower zuweist, finden Sie unter. Überlegungen zu Ressourcen für Account Factory

Interagieren Sie mit AWS Control Tower Tower-Konten von AWS Service Catalog

In diesem Abschnitt erfahren Sie, wie Sie Ihre AWS Control Tower Tower-Konten mit den Funktionen von verwalten AWS Service Catalog.

Themen

- Stellen Sie Konten in der Service Catalog-Konsole mit Account Factory bereit
- Automatisieren Sie die Kontobereitstellung in AWS Control Tower mithilfe von Service Catalog-APIs
- Aktualisieren Sie das bereitgestellte Produkt im Service Catalog
- Ein Konto im Service Catalog deregistrieren

Stellen Sie Konten in der Service Catalog-Konsole mit Account Factory bereit

Im folgenden Verfahren wird beschrieben, wie Sie Konten als Benutzer in IAM Identity Center erstellen und bereitstellen. AWS Service Catalog Dieses Verfahren wird auch als erweiterte Kontobereitstellung oder manuelle Kontobereitstellung bezeichnet. Optional können Sie AWS Control Tower-Konten möglicherweise programmgesteuert, mit der AWS CLI, mit Service Catalog-APIs oder mit AWS Control Tower Account Factory for Terraform (AFT) bereitstellen. Möglicherweise können Sie benutzerdefinierte Konten in der Konsole bereitstellen, wenn Sie zuvor benutzerdefinierte Blueprints eingerichtet haben. Weitere Informationen zur Anpassung finden Sie unterPassen Sie Konten mit Account Factory Customization (AFC) an.

> **Note**
>
> Wenn Sie IAM Identity Center in Ihren landing zone Zone-Einstellungen deaktiviert haben, werden die SSO-Benutzerparameter (`SSOUserEmail`SSOUserFirstName,

undSSOUserLastName) bei der Kontobereitstellung nicht verwendet. Falls gewünscht, können Sie Platzhalterwerte für diese erforderlichen Parameter angeben und sie später ändern, indem Sie den Anweisungen unter folgen. Aktualisieren Sie das bereitgestellte Produkt im Service Catalog

Um Konten einzeln in Account Factory als Benutzer bereitzustellen

1. Melden Sie sich über die URL des Benutzerportals an.
2. Wählen Sie unter „Ihre Anwendungen“ die Option AWS Konto aus.
3. Wählen Sie aus der Liste der Konten die Konto-ID für Ihr Verwaltungskonto aus. Diese ID kann auch eine Bezeichnung haben, zum Beispiel (Management).
4. Wählen Sie AWSServiceCatalogEndUserAccessunter Managementkonsole aus. Dadurch wird das AWS-Managementkonsole für diesen Benutzer in diesem Konto geöffnet.
5. Stellen Sie sicher, dass Sie die richtigen Konten AWS-Region für die Bereitstellung ausgewählt haben. Dies sollte Ihre AWS Control Tower Tower-Region sein.
6. Suchen Sie nach Service Catalog und wählen Sie ihn aus, um die Service Catalog-Konsole zu öffnen.
7. Wählen Sie im Navigationsbereich Produkte aus.
8. Wählen Sie AWS Control Tower Account Factory und dann die Schaltfläche Produkt starten. Damit wird der Assistent für die Bereitstellung eines neuen Kontos gestartet.
9. Fügen Sie die Informationen ein und beachten Sie dabei Folgendes:

   - Dabei SSOUserEmailkann es sich um eine neue E-Mail-Adresse oder um die E-Mail-Adresse handeln, die einem vorhandenen IAM Identity Center-Benutzer zugeordnet ist. Ganz gleich, wofür Sie sich entscheiden, dieser Benutzer hat administrativen Zugriff auf das Konto, das Sie bereitstellen.
   - Bei der AccountEmailmuss es sich um eine E-Mail-Adresse handeln, die noch nicht mit einer AWS-Konto verknüpft ist. Wenn Sie in eine neue E-Mail-Adresse verwendet haben SSOUserEmail, können Sie diese E-Mail-Adresse hier verwenden.

10. Definieren TagOptionsund aktivieren Sie keine Benachrichtigungen, da das Konto sonst möglicherweise nicht bereitgestellt werden kann. Wenn Sie fertig sind, wählen Sie Produkt starten.
11. Überprüfen Sie die Kontoeinstellungen, und wählen Sie dann Launch (Start) aus. Erstellen Sie keinen Ressourcenplan, da das Konto sonst nicht bereitgestellt werden kann.

12. Das Konto wird jetzt bereitgestellt. Dieser Vorgang kann einige Minuten in Anspruch nehmen. Sie können die Seite aktualisieren, um den angezeigten Status zu aktualisieren.

> **Note**
>
> Es können bis zu fünf Konten gleichzeitig bereitgestellt werden.

Automatisieren Sie die Kontobereitstellung in AWS Control Tower mithilfe von Service Catalog-APIs

AWS Control Tower ist in mehrere andere AWS Services integriert, wie AWS Service Catalog z. Sie können die APIs verwenden, um Ihre Mitgliedskonten in AWS Control Tower zu erstellen und bereitzustellen oder um bestehende Mitgliedskonten zu registrieren.

> **Note**
>
> Wenn Sie IAM Identity Center in Ihren landing zone Zone-Einstellungen deaktiviert haben, werden die SSO-Benutzerparameter (`SSOUserEmail`SSOUserFirstName, und`SSOUserLastName`) bei der Kontobereitstellung nicht verwendet. Falls gewünscht, können Sie Platzhalterwerte für diese erforderlichen Parameter angeben und sie später ändern, indem Sie den Anweisungen unter folgen. Aktualisieren Sie das bereitgestellte Produkt im Service Catalog

Das Video zeigt Ihnen, wie Sie Konten automatisiert und stapelweise bereitstellen, indem Sie die AWS Service Catalog APIs aufrufen. Für die Bereitstellung rufen Sie die `ProvisionProduct`API über die AWS Befehlszeilenschnittstelle (CLI) auf und geben eine JSON-Datei an, die die Parameter für jedes Konto enthält, das Sie einrichten möchten. Das Video zeigt die Installation und Verwendung der AWS Cloud9-Entwicklungsumgebung für diese Arbeit. Die CLI-Befehle wären dieselben, wenn Sie AWS Cloudshell anstelle von AWS Cloud9 verwenden.

> **Note**
>
> Sie können diesen Ansatz auch für die Automatisierung von Kontoaktualisierungen anpassen, indem Sie AWS Service Catalog für jedes Konto die

`UpdateProvisionedProduct`API von aufrufen. Sie können ein Skript schreiben, um die Konten nacheinander zu aktualisieren.

Als völlig andere Automatisierungsmethode können Sie, wenn Sie mit Terraform vertraut sind, Konten mit AWS Control Tower Account Factory for Terraform (AFT) bereitstellen.

Beispiel für eine Verwaltungsrolle im Bereich Automatisierung

Hier ist eine Beispielvorlage, die Sie verwenden können, um Ihre Automatisierungsadministratorrolle im Verwaltungskonto zu konfigurieren. Sie würden diese Rolle in Ihrem Verwaltungskonto so konfigurieren, dass sie die Automatisierung mit Administratorzugriff in den Zielkonten durchführen kann.

```
AWSTemplateFormatVersion: 2010-09-09
Description: Configure the SampleAutoAdminRole

Resources:
  AdministrationRole:
    Type: AWS::IAM::Role
    Properties:
      RoleName: SampleAutoAdminRole
      AssumeRolePolicyDocument:
        Version: 2012-10-17
        Statement:
          - Effect: Allow
            Principal:
              Service: cloudformation.amazonaws.com
            Action:
              - sts:AssumeRole
      Path: /
      Policies:
        - PolicyName: AssumeSampleAutoAdminRole
          PolicyDocument:
            Version: 2012-10-17
            Statement:
              - Effect: Allow
                Action:
                  - sts:AssumeRole
                Resource:
                  - "arn:aws:iam::*:role/SampleAutomationExecutionRole"
```

Beispiel für eine Rolle zur Ausführung der Automatisierung

Im Folgenden finden Sie eine Beispielvorlage, mit der Sie die Automatisierungsausführungsrolle einrichten können. Sie würden diese Rolle in den Zielkonten konfigurieren.

```
AWSTemplateFormatVersion: "2010-09-09"
Description: "Create automation execution role for creating Sample Additional Role."

Parameters:
  AdminAccountId:
    Type: "String"
    Description: "Account ID for the administrator account (typically management,
 security or shared services)."
  AdminRoleName:
    Type: "String"
    Description: "Role name for automation administrator access."
    Default: "SampleAutomationAdministrationRole"
  ExecutionRoleName:
    Type: "String"
    Description: "Role name for automation execution."
    Default: "SampleAutomationExecutionRole"
  SessionDurationInSecs:
    Type: "Number"
    Description: "Maximum session duration in seconds."
    Default: 14400

Resources:
  # This needs to run after AdminRoleName exists.
  ExecutionRole:
    Type: "AWS::IAM::Role"
    Properties:
      RoleName: !Ref ExecutionRoleName
      MaxSessionDuration: !Ref SessionDurationInSecs
      AssumeRolePolicyDocument:
        Version: "2012-10-17"
        Statement:
          - Effect: "Allow"
            Principal:
              AWS:
                - !Sub "arn:aws:iam::${AdminAccountId}:role/${AdminRoleName}"
            Action:
              - "sts:AssumeRole"
      Path: "/"
      ManagedPolicyArns:
```

```
        - "arn:aws:iam::aws:policy/AdministratorAccess"
```

Nachdem Sie diese Rollen konfiguriert haben, rufen Sie die AWS Service Catalog APIs auf, um die automatisierten Aufgaben auszuführen. Die CLI-Befehle sind im Video angegeben.

Beispiel für eine Bereitstellungseingabe für die Service Catalog API

Hier ist ein Beispiel für die Eingabe, die Sie an die Service `ProvisionProduct` Catalog-API geben können, wenn Sie die API verwenden, um neue AWS Control Tower Tower-Konten bereitzustellen oder bestehende Mitgliedskonten zu registrieren:

> **Note**
>
> Um ein vorhandenes Mitgliedskonto mithilfe der `ProvisionProduct` API zu registrieren, muss die `AWSControlTowerExecution` IAM-Rolle auf dem Zielkonto vorhanden sein, bevor Sie die API aufrufen. Sie können dieselben Eingabeparameter wie im folgenden Beispiel sowohl für die Bereitstellung neuer Konten als auch für die Registrierung vorhandener Konten verwenden.

```
{
  pathId: "lpv2-7n2o3nudljh4e",
  productId: "prod-y422ydgjge2rs",
  provisionedProductName: "Example product 1",
  provisioningArtifactId: "pa-2mmz36cfpj2p4",
  provisioningParameters: [
    {
      key: "AccountEmail",
      value: "abc@amazon.com"
    },
    {
      key: "AccountName",
      value: "ABC"
    },
    {
      key: "ManagedOrganizationalUnit",
      value: "Custom (ou-xfe5-a8hb8ml8)"
    },
    {
      key: "SSOUserEmail",
      value: "abc@amazon.com"
```

```
    },
    {
      key: "SSOUserFirstName",
      value: "John"
    },
    {
      key: "SSOUserLastName",
      value: "Smith"
    }
  ],
  provisionToken: "c3c795a1-9824-4fb2-a4c2-4b1841be4068"
}
```

Weitere Informationen finden Sie in der API-Referenz für Service Catalog.

> **Note**
>
> Beachten Sie, dass sich das Format der Eingabezeichenfolge für den Wert von von von von `OU_NAME` geändert `ManagedOrganizationalUnit` hat`OU_NAME (OU_ID)`. Im folgenden Video wird diese Änderung nicht erwähnt.

Video-Anleitung

In diesem Video (6:58) wird beschrieben, wie Kontobereitstellungen in AWS Control Tower automatisiert werden. Wählen Sie zur besseren Ansicht das Symbol in der rechten unteren Ecke des Videos, um es in voller Bildschirmgröße anzuzeigen. Es stehen Untertitel zur Verfügung.

Videoanleitung zur automatisierten Kontobereitstellung in AWS Control Tower.

Aktualisieren Sie das bereitgestellte Produkt im Service Catalog

Das folgende Verfahren führt Sie durch die Aktualisierung Ihres Kontos in Account Factory oder die Umstellung auf eine neue Organisationseinheit, indem Sie das für das Konto bereitgestellte Produkt im Service Catalog aktualisieren.

> **Note**
>
> Wenn Sie IAM Identity Center in Ihren landing zone Zone-Einstellungen deaktiviert haben, werden die SSO-Benutzerparameter (`SSOUserEmailSSOUserFirstName`,

undSSOUserLastName) bei der Kontobereitstellung nicht verwendet. Falls gewünscht, können Sie Platzhalterwerte für diese erforderlichen Parameter angeben und sie später ändern, indem Sie den Anweisungen in diesem Abschnitt folgen.

Um ein Account Factory zu aktualisieren oder seine Organisationseinheit über den Service Catalog zu ändern

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die AWS Service Catalog Konsole unter https://console.aws.amazon.com/servicecatalog/.

   > **Note**
   >
   > Sie müssen sich als Benutzer mit Berechtigungen zur Bereitstellung neuer Produkte in Service Catalog anmelden (z. B. als IAM Identity Center-Benutzer in `AWSAccountFactory` oder `AWSServiceCatalogAdmins` Gruppen).

2. Wählen Sie im Navigationsbereich Provisioning und dann Provisioned Products aus.
3. Führen Sie für jedes der aufgelisteten Mitgliedskonten die folgenden Schritte aus, um alle Mitgliedskonten zu aktualisieren:

   a. Wählen Sie ein Mitgliedskonto aus. Sie werden zur Seite mit den bereitgestellten Produktdetails für dieses Konto weitergeleitet.

   b. Wählen Sie auf der Seite mit den Produktdetails zur Bereitstellung den Tab Ereignisse aus.

   c. Notieren Sie die folgenden Parameter:

      - SSOUserEmail(Verfügbar in den Produktdetails für bereitgestellte Produkte)
      - AccountEmail(In den bereitgestellten Produktdetails verfügbar)
      - SSOUserFirstName(Verfügbar im IAM Identity Center)
      - SSOUSerLastName(Verfügbar im IAM Identity Center)
      - AccountName(Verfügbar im IAM Identity Center)

   d. Wählen Sie unter Actions (Aktionen) die Option Update (Aktualisieren) aus.

   e. Wählen Sie die Schaltfläche neben der Version des Produkts, das Sie aktualisieren möchten, und klicken Sie dann auf Next (Weiter).

   f. Geben Sie die bereits erwähnten Parameterwerte an.

- Wenn Sie die bestehende Organisationseinheit behalten möchten, wählen Sie die Organisationseinheit aus ManagedOrganizationalUnit, in der sich das Konto bereits befand.
- Wenn Sie das Konto auf eine neue Organisationseinheit migrieren möchten ManagedOrganizationalUnit, wählen Sie die neue Organisationseinheit für das Konto aus.

Ein zentraler Cloud-Administrator kann diese Informationen in der AWS Control Tower Tower-Konsole auf der Seite Organisation finden.

g. Wählen Sie Weiter aus.

h. Überprüfen Sie die Änderungen und klicken Sie dann auf Update (Aktualisieren). Dieser Vorgang kann pro Konto einige Minuten in Anspruch nehmen.

Ein Konto im Service Catalog deregistrieren

Die Registrierung eines Kontos kann in der Service Catalog-Konsole von einem IAM Identity Center-Benutzer in der `AWSAccountFactory` Gruppe aufgehoben werden, indem das bereitgestellte Produkt beendet wird. Weitere Informationen zu Benutzern oder Gruppen von IAM Identity Center finden Sie unter Benutzer und Zugriff verwalten über. AWS IAM Identity Center Das folgende Verfahren beschreibt, wie Sie ein Mitgliedskonto im Service Catalog abmelden.

So heben Sie die Registrierung eines registrierten Kontos über Service Catalog auf

1. Öffnen Sie die Service Catalog-Konsole in Ihrem Webbrowser unterhttps://console.aws.amazon.com/servicecatalog.
2. Wählen Sie im linken Navigationsbereich die Option Liste der bereitgestellten Produkte aus.
3. Wählen Sie aus der Liste der bereitgestellten Konten den Namen des Kontos aus, das AWS Control Tower nicht mehr verwalten soll.
4. Wählen Sie auf der Seite Provisioned products details (Details der bereitgestellten Produkte) im Menü Actions (Aktionen) die Option Terminate (Beenden) aus.
5. Wählen Sie im angezeigten Dialogfeld die Option Terminate (Beenden) aus.

> **Important**
>
> Das Wort beenden ist spezifisch für Service Catalog. Wenn Sie ein Konto in Service Catalog Account Factory kündigen, wird das Konto nicht geschlossen. Durch diese Aktion wird das Konto aus seiner Organisationseinheit und Ihrer landing zone entfernt.

6. Wenn das Konto deregistriert wurde, ändert sich sein Status in Nicht aktiviert.
7. Wenn Sie das Konto nicht mehr benötigen, schließen Sie es. Weitere Informationen zum Schließen von AWS Konten finden Sie im AWS Billing Benutzerhandbuch unter Schließen eines Kontos

> **Note**
>
> Warten Sie, bis der Status des Kontos Nicht aktiviert angezeigt wird.

Bereitstellung und Verwaltung von Konten im AWS Control Tower

Dieses Kapitel beinhaltet:

- eine Übersicht und Verfahren für die Bereitstellung und Verwaltung neuer Mitgliedskonten in AWS Control Tower.
- eine Übersicht und Verfahren für die Registrierung eines bestehenden AWS Kontos bei AWS Control Tower.

Allgemeine Informationen zu Konten in AWS Control Tower finden Sie unterInformationen AWS-Konten im AWS Control Tower. Informationen zur Registrierung mehrerer Konten bei AWS Control Tower finden Sie unter. Registrieren Sie eine bestehende Organisationseinheit bei AWS Control Tower

> **Note**
>
> Die Bereitstellung, Aktualisierung und Anpassung eines einzelnen Kontos muss auf eine Organisationseinheit (OU) abzielen, die aktiviert ist. AWSControlTowerBaseline Wenn für eine Organisationseinheit diese Option nicht AWSControlTowerBaseline aktiviert ist, können Sie die automatische Kontoregistrierung aktivieren oder zur Kontoregistrierung ResetEnabledBaseline beliebige ResetEnabledControl APIs auf EnabledBaselines und EnabledControls auf dieser Organisationseinheit verwenden. Einzelheiten finden Sie unter:. AWSControlTowerBaseline Basistypen, die auf OU-Ebene gelten

> **Note**
>
> Sie können bis zu fünf (5) kontobezogene Vorgänge gleichzeitig ausführen, einschließlich Bereitstellung, Aktualisierung und Registrierung.

Für die Bereitstellung von Konten sind Berechtigungen erforderlich

Mit den entsprechenden Benutzergruppenberechtigungen können Provisioner standardisierte Basislinien und Netzwerkkonfigurationen für alle Konten in ihrer Organisation angeben.

Wenn Sie Konten von der AWS Control Tower-Konsole aus mit Account Factory erstellen, müssen Sie bei einem Konto mit einem IAM-Benutzer angemeldet sein, für den die `AWSServiceCatalogEndUserFullAccess` Richtlinie sowie die Berechtigungen zur Nutzung der AWS Control Tower-Konsole aktiviert sind. Sie können nicht als Root-Benutzer angemeldet sein.

> **Note**
>
> Bei der Bereitstellung eines Kontos muss der Kontoantragsteller immer über die Berechtigungen `CreateAccount` und die Berechtigungen verfügen. `DescribeCreateAccountStatus` Dieser Berechtigungssatz ist Teil der Admin-Rolle und wird automatisch vergeben, wenn ein Anforderer die Admin-Rolle übernimmt. Wenn Sie die Berechtigung zur Bereitstellung von Konten delegieren, müssen Sie diese Berechtigungen möglicherweise direkt für die Kontoanforderer hinzufügen.

Allgemeine Informationen zu den im AWS Control Tower erforderlichen Berechtigungen finden Sie unter. Verwenden identitätsbasierter Richtlinien (IAM-Richtlinien) für AWS Control Tower Informationen zu Rollen und Konten in AWS Control Tower finden Sie unter Rollen und Konten.

Stellen Sie Konten innerhalb von AWS Control Tower bereit

AWS Control Tower bietet verschiedene Methoden zum Erstellen und Aktualisieren von Mitgliedskonten. Einige Methoden basieren hauptsächlich auf Konsolen, und einige Methoden sind hauptsächlich automatisiert.

Übersicht

Eine Standardmethode zur Erstellung von Mitgliedskonten im AWS Control Tower ist Account Factory, ein konsolenbasiertes Produkt, das Teil des Service Catalogs ist. Außerdem können Sie von der AWS Control Tower-Konsole aus Konto erstellen als Methode für die Bereitstellung neuer Konten verwenden. Außerdem können Sie Konto registrieren verwenden, um bestehende AWS Konten bei AWS Control Tower zu registrieren, falls sich Ihre Landezone nicht gerade im Trend befindet.

Mit Account Factory können Sie Basiskonten bereitstellen, wobei Sie sich auf die Standardeinstellungen des AWS Control Tower verlassen. Sie können auch benutzerdefinierte Konten bereitstellen, die die Anforderungen für spezielle Anwendungsfälle erfüllen.

Account Factory Customization (AFC) ist eine Methode zur Bereitstellung benutzerdefinierter Konten von der AWS Control Tower-Konsole aus und automatisiert die Anpassung und Bereitstellung Ihrer Konten. Es ermöglicht eine konsolenbasierte, automatisierte Bereitstellung nach einigen einmaligen Einrichtungsschritten, sodass Sie keine Skripte schreiben oder Pipelines einrichten müssen. Weitere Informationen finden Sie unter Passen Sie Konten mit Account Factory Customization (AFC) an.

> **Automatische Registrierung**
>
> Sie können sie auch AWS-Konten außerhalb von AWS Control Tower erstellen und sie in eine OU verschieben, die bei AWS Control Tower registriert ist, ohne dass es zu einer Vererbung kommt, wenn Sie in Ihren Landingzone-Einstellungen die Funktion Automatisierte Kontoregistrierung aktivieren. Weitere Informationen finden Sie unter Konten mit automatischer Registrierung verschieben und registrieren.

Console-based Methoden:

- Über die Account Factory-Konsole, die Teil von ist AWS Service Catalog, für einfache oder benutzerdefinierte Konten. Bereitstellung und Verwaltung von Konten mit Account FactoryEinzelheiten und Anweisungen finden Sie hier.
- Durch automatische Registrierung, indem ein Konto von der Konsole aus in eine OU verschoben wird. Siehe Konten mit automatischer Registrierung verschieben und registrieren
- Über die Funktion Konto registrieren im AWS Control Tower, wenn sich Ihre Landezone nicht gerade im Driftzustand befindet. Siehe Registrieren Sie ein vorhandenes Konto über die AWS Control Tower-Konsole.
- In der AWS Control Tower-Konsole können Sie Account Factory verwenden, um bis zu fünf Konten gleichzeitig zu erstellen, zu aktualisieren oder zu registrieren.

Automatisierte Methoden:

- Lambda-Code: Vom Verwaltungskonto Ihrer AWS Control Tower-Landingzone aus, mithilfe von Lambda-Code und den entsprechenden IAM-Rollen. Siehe Automatisierte Kontobereitstellung mit IAM-Rollen.
- Terraform: Aus der AWS Control Tower Account Factory for Terraform (AFT), die auf Account Factory und einem GitOps Modell basiert, das die Automatisierung der Kontobereitstellung und -aktualisierung ermöglicht. Siehe Bereitstellung von Konten mit AWS Control Tower Account Factory für Terraform (AFT).

- Durch automatische Registrierung, indem ein vorhandenes Konto mithilfe von APIs in eine OU verschoben wird. Siehe Konten mit automatischer Registrierung verschieben und registrieren
- Account Factory-Anpassung in der AWS Control Tower-Konsole: Nach den Einrichtungsschritten erfordert die zukünftige Bereitstellung benutzerdefinierter Konten keine zusätzliche Konfiguration oder Pipeline-Wartung. Konten werden mithilfe eines AWS Service Catalog Produkts bereitgestellt, das als Blueprint bezeichnet wird. Ein Blueprint kann Vorlagen oder CloudFormation Terraform-Vorlagen verwenden.

> **Note**
>
> CloudFormation Blueprints können Ressourcen in mehreren Regionen bereitstellen. Terraform-Blueprints können Ressourcen nur in einer einzigen Region bereitstellen. Standardmäßig ist dies die Heimatregion.

Konten in der AWS Control Tower Tower-Konsole bereitstellen

Das folgende Verfahren beschreibt, wie Sie Konten als Benutzer im IAM Identity Center über die AWS Control Tower Tower-Konsole erstellen und bereitstellen. Dieses Verfahren wird auch als manuelle Kontobereitstellung bezeichnet. Optional können Sie AWS Control Tower-Konten programmgesteuert, mit der AWS CLI, mit Service Catalog APIs oder mit AWS Control Tower Account Factory for Terraform (AFT) bereitstellen oder ein vorhandenes Konto automatisch bei einer registrierten OU registrieren. Möglicherweise können Sie benutzerdefinierte Konten in der Konsole bereitstellen, wenn Sie zuvor benutzerdefinierte Blueprints eingerichtet haben. Weitere Informationen zur Anpassung finden Sie unterPassen Sie Konten mit Account Factory Customization (AFC) an.

Um Konten als Benutzer einzeln in der AWS Control Tower Tower-Konsole bereitzustellen

1. Melden Sie sich an AWS und navigieren Sie zur AWS Control Tower Tower-Konsole.
2. Wählen Sie in der linken Navigationsleiste Organizations aus, um die Seite Organisation aufzurufen.
3. Wählen Sie oben rechts Ressourcen erstellen aus.
4. Wählen Sie im Drop-down-Menü die Option Konto erstellen.
5. Geben Sie die Informationen auf der Seite ein und beachten Sie dabei Folgendes:

    - Die Konto-E-Mail-Adresse muss eine E-Mail-Adresse sein, die noch nicht mit einer verknüpft ist AWS-Konto.

- Der Anzeigename ist der Name, den Sie für dieses Konto sehen möchten.

6. Füllen Sie die Felder aus, um Ihre Access-Konfiguration mit einer IAM Identity Center-E-Mail-Adresse und einem Benutzernamen zu definieren.
7. Wählen Sie eine registrierte OU aus der Drop-down-Liste aus, um die OU anzugeben, in der Sie das Konto bereitstellen möchten.
8. Verwenden Sie optional einen vordefinierten Blueprint, um Ihrem Konto maßgeschneiderte Ressourcen zur Verfügung zu stellen. Sie können diese Aufgabe später erledigen.
9. Überprüfen Sie Ihre Kontoauswahl und wählen Sie dann unten rechts Konto erstellen aus.
10. Das Konto wird jetzt bereitgestellt. Dieser Vorgang kann einige Minuten in Anspruch nehmen. Sie können die Seite aktualisieren, um den angezeigten Status zu aktualisieren.

> **Note**
>
> Es können bis zu fünf Konten gleichzeitig bereitgestellt werden.

Sehen Sie sich Ihre Konten an

Auf der Seite Organisation werden alle Organisationseinheiten und Konten in Ihrer Organisation aufgeführt, unabhängig von der Organisationseinheit oder dem Registrierungsstatus im AWS Control Tower. Sie können Mitgliedskonten — einzeln oder nach OU-Gruppen — im AWS Control Tower einsehen und registrieren, sofern jedes Konto die Voraussetzungen für die Registrierung erfüllt.

Um ein bestimmtes Konto einzusehen

- Navigieren Sie zur Seite „Organisation“.
- Sie können im Drop-down-Menü oben rechts die Option Nur Konten auswählen.
- Wählen Sie dann den Namen Ihres Kontos aus der Tabelle aus.
- Sie können auch den Namen der übergeordneten Organisationseinheit aus der Tabelle auswählen und auf der Detailseite für diese Organisationseinheit eine Liste aller Konten innerhalb dieser Organisationseinheit anzeigen.

Auf der Seite „Organisation“ und der Seite „Kontodetails“ können Sie den Status des Kontos sehen. Dieser ist einer der folgenden:

- Nicht registriert — Das Konto ist Mitglied der übergeordneten Organisationseinheit, wird jedoch nicht vollständig von AWS Control Tower verwaltet. Wenn die übergeordnete OU registriert ist, unterliegt das Konto den präventiven Kontrollen, die für die registrierte übergeordnete OU konfiguriert sind, aber die Detective Controls der OU gelten nicht für dieses Konto. Wenn die übergeordnete Organisationseinheit nicht registriert ist, gelten für dieses Konto keine Kontrollen.
- Registrierung — Das Konto wird derzeit vom AWS Control Tower verwaltet. Wir stimmen das Konto mit der Kontrollkonfiguration für die übergeordnete OU ab. Dieser Vorgang kann mehrere Minuten pro Kontoressource in Anspruch nehmen.
- Eingeschrieben — Das Konto unterliegt den Steuerelementen, die für die übergeordnete Organisationseinheit konfiguriert sind. Es wird vollständig vom AWS Control Tower verwaltet.
- Registrierung fehlgeschlagen — Das Konto konnte nicht bei AWS Control Tower registriert werden. Weitere Informationen finden Sie unter Häufige Ursachen für das Scheitern der Registrierung.
- Update verfügbar — Für das Konto ist ein Update verfügbar. Konten in diesem Status sind immer noch registriert, aber das Konto muss aktualisiert werden, um die letzten Änderungen an Ihrer Umgebung widerzuspiegeln. Um ein einzelnes Konto zu aktualisieren, navigieren Sie zur Kontodetailseite und wählen Sie Konto aktualisieren aus.

  Wenn Sie mehrere Konten mit diesem Status unter einer einzigen Organisationseinheit haben, können Sie Re-register die Organisationseinheit auswählen und diese Konten zusammen aktualisieren.

Über das Registrieren vorhandener Konten

Sie können die AWS Control Tower-Governance auf eine Einzelperson ausdehnen. Diese besteht bereits, AWS-Konto wenn Sie sie in eine Organisationseinheit (OU) aufnehmen, die bereits von AWS Control Tower verwaltet wird. Teilnahmeberechtigte Konten befinden sich in nicht registrierten Organisationseinheiten, die Teil derselben AWS Organizations Organisation wie die AWS Control Tower-OU sind.

Für die Registrierung von Konten bei AWS Control Tower gibt es mehrere Methoden. Die Informationen auf dieser Seite gelten für alle Registrierungsmethoden.

> **Note**
>
> Sie können ein bestehendes AWS Konto nicht als Audit- oder Protokollarchivkonto registrieren, außer bei der ersten Einrichtung der Landezone.

Was passiert bei der Kontoregistrierung

Während des Registrierungsprozesses führt AWS Control Tower die folgenden Aktionen durch:

- Grundlegende Erstellung des Kontos, darunter die Bereitstellung dieser Stack-Sets:
  - `AWSControlTowerBP-BASELINE-CLOUDTRAIL`
  - `AWSControlTowerBP-BASELINE-CLOUDWATCH`
  - `AWSControlTowerBP-BASELINE-CONFIG`
  - `AWSControlTowerBP-BASELINE-ROLES`
  - `AWSControlTowerBP-BASELINE-SERVICE-ROLES`
  - `AWSControlTowerBP-BASELINE-SERVICE-LINKED-ROLES`
  - `AWSControlTowerBP-VPC-ACCOUNT-FACTORY-V1`

  Es empfiehlt sich, die Vorlagen dieser Stack-Sets zu überprüfen und sicherzustellen, dass sie nicht mit Ihren bestehenden Richtlinien in Konflikt stehen.
- Identifiziert das Konto durch AWS IAM Identity Center oder. AWS Organizations
- Platziert des Kontos in der von Ihnen angegebenen OU. Stellen Sie sicher, dass SCPs in der aktuellen OUs angewendet werden, damit Ihre Sicherheitsposition konsistent bleibt.
- Wendet mithilfe der SCPs, die für die gesamte ausgewählte Organisationseinheit gelten, obligatorische Kontrollen auf das Konto an.
- Aktiviert AWS Config und konfiguriert es so, dass alle Ressourcen im Konto aufgezeichnet werden.
- Fügt die AWS Config Regeln hinzu, die die Detektivkontrollen von AWS Control Tower auf das Konto anwenden.

> **Konten und Pfade auf Organisationsebene CloudTrail**
>
> Für Landing Zone-Versionen 3.1 und höher gilt Folgendes, wenn Sie die optionale AWS CloudTrail Integration in den Landezone-Einstellungen ausgewählt haben:

- Für alle Mitgliedskonten in einer OU gilt der Tarif für die AWS CloudTrail OU, unabhängig davon, ob sie registriert sind oder nicht.
- Wenn Sie ein Konto bei AWS Control Tower registrieren, unterliegt Ihr Konto dem AWS CloudTrail Trail für die neue Organisation. Wenn Sie bereits über eine Bereitstellung eines CloudTrail Trails verfügen, fallen möglicherweise doppelte Gebühren an, es sei denn, Sie löschen den vorhandenen Trail für das Konto, bevor Sie es bei AWS Control Tower registrieren.
- Wenn Sie ein Konto in eine registrierte Organisationseinheit verschieben — zum Beispiel über die AWS Organizations Konsole oder APIs — möchten Sie möglicherweise alle verbleibenden Trails für das Konto entfernen. Wenn du bereits einen CloudTrail Trail installiert hast, fallen für dich doppelte Gebühren an. CloudTrail

Wenn du deine Landezone aktualisierst und dich dafür entscheidest, Trails auf Organisationsebene abzubestellen, oder wenn deine Landezone älter als Version 3.0 ist, gelten die CloudTrail Trails auf Organisationsebene nicht für deine Konten.

Registrieren Sie bestehende Konten bei VPCs

AWS Control Tower behandelt VPCs anders, wenn Sie ein neues Konto in Account Factory bereitstellen, als wenn Sie ein vorhandenes Konto registrieren.

- Wenn Sie ein neues Konto erstellen, entfernt AWS Control Tower automatisch die AWS Standard-VPC und erstellt eine neue VPC für dieses Konto.
- Wenn Sie ein vorhandenes Konto registrieren, erstellt AWS Control Tower keine neue VPC für dieses Konto.
- Wenn Sie ein vorhandenes Konto registrieren, entfernt AWS Control Tower keine vorhandene VPC oder AWS Standard-VPC, die mit dem Konto verknüpft sind.

Tip

Sie können das Standardverhalten für neue Konten ändern, indem Sie Account Factory so konfigurieren, dass für Konten in Ihrer Organisation unter AWS Control Tower nicht

standardmäßig eine VPC eingerichtet wird. Weitere Informationen finden Sie unter Erstellen Sie ein Konto in AWS Control Tower ohne VPC.

Registrieren Sie Konten bei AWS Config Ressourcen

Das Konto, das registriert werden soll, darf über keine vorhandenen AWS Config Ressourcen verfügen. Weitere Informationen finden Sie unter Konten registrieren, die über vorhandene AWS Config Ressourcen verfügen.

Im Folgenden finden Sie einige AWS Config CLI-Beispielbefehle, mit denen Sie den Status der AWS Config Ressourcen Ihres bestehenden Kontos ermitteln können, z. B. des Konfigurationsrekorders und des Bereitstellungskanals.

Befehle anzeigen:

- `aws configservice describe-delivery-channels`
- `aws configservice describe-delivery-channel-status`
- `aws configservice describe-configuration-recorders`

Die normale Antwort ist etwa so `"name": "default"`

Befehle löschen:

- `aws configservice stop-configuration-recorder --configuration-recorder-name` *`NAME-FROM-DESCRIBE-OUTPUT`*
- `aws configservice delete-delivery-channel --delivery-channel-name` *`NAME-FROM-DESCRIBE-OUTPUT`*
- `aws configservice delete-configuration-recorder --configuration-recorder-name` *`NAME-FROM-DESCRIBE-OUTPUT`*

Voraussetzungen für die Immatrikulation

In diesem Abschnitt wird beschrieben, wie Sie ein vorhandenes AWS Konto bei AWS Control Tower registrieren, wenn Sie auf der Seite mit den Landingzone-Einstellungen nicht die optionale Funktion zur automatischen Registrierung ausgewählt haben oder wenn Sie mit einer Landing Zone-Version vor 3.1 arbeiten.

Diese Voraussetzungen sind erforderlich, bevor Sie ein vorhandenes AWS-Konto bei AWS Control Tower registrieren können:

> **Note**
>
> Die Voraussetzung für das Hinzufügen der `AWSControlTowerExecution` Rolle ist nicht erforderlich, wenn Sie die Funktion zur automatischen Registrierung im AWS Control Tower auf der Seite mit den Landing Zone-Einstellungen aktiviert haben oder wenn Sie das Konto im Rahmen einer Registrierung einer Organisationseinheit registrieren. In allen Fällen verfügt das Konto, das registriert werden soll, jedoch möglicherweise nicht über vorhandene Ressourcen. AWS Config Siehe Konten registrieren, die über vorhandene Ressourcen verfügen AWS Config

1. Um ein vorhandenes Konto zu registrieren AWS-Konto, muss die `AWSControlTowerExecution` Rolle in dem Konto vorhanden sein, das Sie registrieren. Einzelheiten und Anweisungen finden Sie unter Konto https://docs.aws.amazon.com/controltower/latest/userguide/quick-account-provisioning.html registrieren.
2. Zusätzlich zur `AWSControlTowerExecution` Rolle muss das Unternehmen, das AWS-Konto Sie registrieren möchten, über die folgenden Berechtigungen und Vertrauensbeziehungen verfügen. Andernfalls schlägt die Anmeldung fehl.

   Rollenberechtigung: `AdministratorAccess` (AWS verwaltete Richtlinie)

   Rolle: Vertrauensverhältnis:

   JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:root"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

3. Wir empfehlen, dass das Konto weder über einen AWS Config Konfigurationsrekorder noch über einen Bereitstellungskanal verfügt. Diese können über das gelöscht oder geändert werden, AWS CLI bevor Sie ein Konto registrieren können. Andernfalls finden Sie unter Konten registrieren, die über vorhandene AWS Config Ressourcen verfügen, Anweisungen, wie Sie Ihre vorhandenen Ressourcen ändern können.
4. Das Konto, das Sie registrieren möchten, muss in derselben AWS Organizations Organisation existieren wie das AWS Control Tower-Managementkonto. Das bestehende Konto kann nur in derselben Organisation wie das AWS Control Tower-Verwaltungskonto registriert werden, und zwar in einer Organisationseinheit, die bereits bei AWS Control Tower registriert ist.

Weitere Voraussetzungen für die Registrierung finden Sie unter Erste Schritte mit AWS Control Tower.

> **Note**
>
> Wenn Sie ein Konto bei AWS Control Tower registrieren, unterliegt Ihr Konto dem Plan für die AWS Control AWS CloudTrail Tower-Organisation. Wenn Sie bereits über eine Bereitstellung eines CloudTrail Trails verfügen, fallen möglicherweise doppelte Gebühren an, es sei denn, Sie löschen den vorhandenen Trail für das Konto, bevor Sie es bei AWS Control Tower registrieren.

Über vertrauenswürdigen Zugriff mit der Rolle **`AWSControlTowerExecution`**

Bevor Sie ein AWS-Konto bestehendes Konto bei AWS Control Tower registrieren können, müssen Sie AWS Control Tower die Erlaubnis geben, das Konto zu verwalten oder zu verwalten. Insbesondere benötigt AWS Control Tower die Erlaubnis, einen vertrauenswürdigen Zugriff zwischen AWS CloudFormation und in AWS Organizations Ihrem Namen einzurichten, damit Ihr Stack automatisch für die Konten in Ihrer ausgewählten Organisation bereitgestellt werden CloudFormation kann. Mit diesem vertrauenswürdigen Zugriff führt die `AWSControlTowerExecution` Rolle Aktivitäten durch, die zur Verwaltung der einzelnen Konten erforderlich sind. Deshalb müssen Sie diese Rolle jedem Konto hinzufügen, bevor Sie es registrieren.

Wenn der vertrauenswürdige Zugriff aktiviert ist, CloudFormation können Stacks für mehrere Konten und AWS-Regionen mit einem einzigen Vorgang erstellt, aktualisiert oder gelöscht werden. AWS Control Tower stützt sich auf diese Vertrauensfunktion, damit es Rollen und Berechtigungen auf

bestehende Konten anwenden kann, bevor es sie in eine registrierte Organisationseinheit verschiebt und sie dadurch der Kontrolle unterstellt.

Weitere Informationen über vertrauenswürdigen Zugriff und AWS CloudFormation StackSets finden Sie unter AWS CloudFormationStackSets und AWS Organizations.

Konten mit automatischer Registrierung verschieben und registrieren

Die Funktion zur automatischen Kontoregistrierung ist für Landezonen der Version 3.1 und höher verfügbar.

Wenn Sie diese Funktion optional aktivieren, können Sie die AWS Organizations APIs und die Konsole verwenden, um Konten in den AWS Control Tower zu verschieben, ohne dass es zu einer Vererbung kommt. Das Konto erhält automatisch Basisressourcen und Kontrollkonfigurationen von der Zielorganisationseinheit (OU) im AWS Control Tower. Diese optionale Funktion ermöglicht es Ihnen auch, Konten innerhalb von AWS Control Tower zwischen Organisationseinheiten zu verschieben, ohne dass es zu einer Vererbungsabweichung kommt, wenn für beide Organisationseinheiten dieselbe Basiskonfiguration und dieselben Steuerelemente aktiviert sind.

Um die automatische Registrierung zu aktivieren: Sie können die automatische Registrierung von Konten auf der Seite mit den Landing Zone-Einstellungen in der AWS Control Tower-Konsole auswählen oder indem Sie den AWS Control Tower oder die `UpdateLandingZone` APIs aufrufen, wobei der Wert des `CreateLandingZone` `RemediationType` Parameters auf Inheritance Drift gesetzt ist.

Um Konten zu registrieren: Nachdem Sie die automatische Registrierung aktiviert haben, verschieben Sie ein Konto mithilfe der Konsole, der API oder der AWS Control AWS Organizations Tower-Konsole in eine registrierte OU. AWS Organizations `MoveAccount` Das Konto erhält automatisch grundlegende Ressourcen und Steuerelemente von dieser OU. Dies gilt sowohl für bestehende Konten als auch für neu erstellte Konten (die standardmäßig im Stammverzeichnis der Organisation erstellt werden).

So heben Sie die Registrierung eines Kontos auf: Verschieben Sie das Konto in eine OU, die nicht bei AWS Control Tower registriert ist, oder in das Stammverzeichnis der Organisation. AWS Control Tower entfernt automatisch alle bereitgestellten Basisressourcen und Kontrollen.

> **Note**
>
> Wenn die Quell- und Ziel-OUs im AWS Control Tower unterschiedliche Konfigurationen haben, kann es zu Abweichungen im Konto Mitgliedskonto wurde verschoben kommen.

Voraussetzungen: Konfiguration für die automatische Registrierung

- Sie müssen die AWS Control Tower Landing Zone Version 3.1 oder höher ausführen.
- Aktivieren Sie die Funktion zur automatischen Registrierung von AWS Control Tower über die Seite mit den Landing Zone-Einstellungen in der Konsole oder über die AWS Control Tower Landing Zone-APIs, indem Sie den Wert des `RemediationTypes` Parameters auf setzen. `Inheritance Drift` Wenn Sie sich angemeldet haben, reagiert der AWS Control Tower in Ihrem Namen sofort auf `move account` Ereignisse und behebt die Vererbungsabweichung für die verschobenen Konten sofort. AWS Organizations

Erforderliche Berechtigungen

Für die Verwendung der API und der AWS Organizations `CreateAccount` API sind bestimmte Rollen und `MoveAccount` Berechtigungen erforderlich. Weitere Informationen zur Verwendung AWS Organizations mit AWS Control Tower finden Sie unter AWS Control Tower und AWS Organizations.

Beispiele für die API-Nutzung

Weitere Informationen und Beispiele zu diesen APIs finden Sie unter `CreateAccount` und `MoveAccount` in der AWS Organizations API-Referenz.

Überlegungen

- Zeitplan für die Registrierung: Ein Konto, das in eine OU verschoben wurde, die bei AWS Control Tower registriert ist, wird mit einem eventuellen Konsistenzmodell registriert. Dieser Vorgang dauert in der Regel einige Minuten, bis zu mehreren Stunden, abhängig von der Anzahl der Konten, die verschoben werden.
- AWS Von Service Catalog bereitgestellte Produkte: Auto-enrollment erstellt, ändert oder beendet keine von AWS Service Catalog bereitgestellten Produkte. Wenn ein Konto zuvor über Account Factory registriert wurde und dem ein bereitgestelltes Produkt zugeordnet ist, verbleibt dieses bereitgestellte Produkt im Verwaltungskonto, nachdem das Konto deregistriert wurde.

Informationen zur Bereinigung verwaister bereitgestellter Produkte finden Sie unter Löschen von bereitgestellten Produkten im Service Catalog-Benutzerhandbuch. AWS

Registrieren Sie ein vorhandenes Konto über die AWS Control Tower-Konsole

Es gibt zwei gängige Methoden, um eine Person für AWS-Konto den AWS Control Tower zu registrieren.

1. Nachdem Sie auf der Seite „Einstellungen“ die Funktion für die automatische Registrierung ausgewählt haben, können Sie eine AWS-Konto außerhalb von AWS Control Tower befindliche Organisationseinheit erstellen und diese direkt in eine registrierte Organisationseinheit verschieben. Weitere Informationen finden Sie unter Automatisches Verschieben und Registrieren von Konten. Diese Option ist für Landing Zone-Versionen 3.1 und höher verfügbar.
2. Sie können ein vorhandenes Konto manuell über die AWS Control Tower-Konsole registrieren.

In den folgenden Abschnitten wird die zweite Option beschrieben, für die keine vorherige Konfiguration Ihrer AWS Control Tower-Umgebung erforderlich ist. Sie AWS-Konto müssen die erforderlichen Voraussetzungen erfüllen.

Sehen Sie sich Ihre berechtigten Konten in der Konsole an:

1. Navigieren Sie im AWS Control Tower zur Seite Organisation.
2. Suchen Sie den Namen des Kontos, das Sie registrieren möchten. Um ihn zu finden, wählen Sie im Dropdownmenü oben rechts die Option Nur Konten aus und suchen Sie dann den Kontonamen in der gefilterten Tabelle.

Folgen Sie als Nächstes den Schritten zur Registrierung eines einzelnen Kontos, wie im Schritte zur manuellen Registrierung eines Kontos Abschnitt gezeigt.

Überlegungen zur Registrierung über die Konsole

- Die Funktion Konto registrieren, die in der AWS Control Tower-Konsole verfügbar ist, ist für die Registrierung vorhandener Konten vorgesehen, AWS-Konten sodass diese vom AWS Control Tower verwaltet werden. Weitere Informationen finden Sie unter Einen bestehenden registrieren. AWS-Konto

- Die konsolenbasierte Funktion „Konto registrieren“ ist verfügbar, wenn sich Ihre Landezone nicht im Drift-Zustand befindet. https://docs.aws.amazon.com/controltower/latest/userguide/drift.html Wenn sich Ihre Landing Zone in einem Abweichungsstatus befindet, können Sie die Funktion Enroll account (Konto anmelden) möglicherweise nicht erfolgreich verwenden. Du musst neue Konten über Account Factory oder eine andere Methode einrichten, bis deine Landing Zone Drift behoben ist.
- Wenn Sie Konten über die AWS Control Tower-Konsole registrieren, müssen Sie bei einem Konto mit einem Benutzer angemeldet sein, für den die `AWSServiceCatalogEndUserFullAccess` Richtlinie aktiviert ist und über Administratorzugriffsberechtigungen für die Nutzung der AWS Control Tower-Konsole verfügt. Sie können nicht als Root-Benutzer angemeldet sein.
- Konten, die Sie registrieren, können mithilfe der AWS Control Tower Account Factory aktualisiert werden, wie Sie jedes andere Konto aktualisieren würden. Aktualisierungsverfahren werden im Abschnitt Konten mit AWS Control Tower aktualisieren und verschieben genannt.

> **Note**
>
> Wenn Sie eine bestehende E-Mail-Adresse registrieren, stellen Sie sicher AWS-Konto, dass Sie die vorhandene E-Mail-Adresse verifizieren. Andernfalls kann ein neues Konto erstellt werden.

Schritte zur manuellen Registrierung eines Kontos

Nachdem die AdministratorAccess Zugriffsberechtigung (Richtlinie) in Ihrem bestehenden AWS-Konto Konto in Kraft getreten ist, gehen Sie wie folgt vor, um das Konto zu registrieren:

Um ein einzelnes Konto von der Konsole aus bei AWS Control Tower zu registrieren

- Navigieren Sie zur Seite AWS Control Tower Organization.
- Auf der Seite „Organisation“ können Sie für Konten, die zur Registrierung berechtigt sind, oben im Abschnitt im Drop-down-Menü „Aktionen“ die Option „Registrieren“ auswählen. Für diese Konten wird außerdem die Schaltfläche Konto registrieren angezeigt, wenn du sie auf der Seite mit den Kontodetails aufrufst.
- Wenn Sie Konto registrieren wählen, wird die Seite Konto registrieren angezeigt, auf der Sie aufgefordert werden, die `AWSControlTowerExecution` Rolle dem Konto hinzuzufügen. Einige Anweisungen finden Sie unter. Fügen Sie die erforderliche IAM-Rolle manuell zu einer vorhandenen hinzu AWS-Konto und registriere es

- Wählen Sie als Nächstes eine registrierte Organisationseinheit aus der Dropdownliste aus. Wenn sich das Konto bereits in einer registrierten OU befindet, wird die OU in dieser Liste angezeigt.
- Wählen Sie Enroll account (Konto anmelden).
- Es wird eine modale Erinnerung angezeigt, in der Sie die `AWSControlTowerExecution` Rolle hinzufügen und die Aktion bestätigen müssen.
- Wählen Sie „Registrieren“.
- AWS Control Tower beginnt mit der Registrierung und Sie werden zurück zur Seite mit den Kontodetails geleitet.

Häufige Ursachen für das Scheitern der Registrierung

- Um ein bestehendes Konto zu registrieren, muss die `AWSControlTowerExecution` Rolle in dem Konto vorhanden sein, das Sie registrieren.
- Ihrem IAM-Prinzipal fehlen die erforderlichen Berechtigungen zum Bereitstellen eines Kontos.
- AWS -Security-Token-Service (AWS STS) ist in Ihrer Heimatregion oder AWS-Konto in jeder Region, die von AWS Control Tower unterstützt wird, deaktiviert.
- Möglicherweise sind Sie als IAM-Benutzer oder als Rolle angemeldet, die dem Account Factory-Portfolio hinzugefügt werden muss. AWS Service Catalog Der Benutzer oder die Rolle muss hinzugefügt werden, bevor Sie Zugriff auf Account Factory erhalten, damit Sie ein Konto bei AWS Control Tower erstellen oder registrieren können. Wenn der entsprechende Benutzer oder die entsprechende Rolle nicht zum Account Factory-Portfolio hinzugefügt wird, erhalten Sie eine Fehlermeldung, wenn Sie versuchen, ein Konto hinzuzufügen. Anweisungen zum Gewähren von Zugriff auf AWS Service Catalog Portfolios finden Sie unter Benutzern Zugriff gewähren.
- Möglicherweise sind Sie als Stammbenutzer angemeldet.
- Das Konto, das Sie registrieren möchten, enthält möglicherweise AWS Config Resteinstellungen. Insbesondere kann das Konto über einen Konfigurationsrekorder oder einen Übertragungskanal verfügen. Diese müssen über das gelöscht oder geändert werden, AWS CLI bevor Sie ein Konto registrieren können. Weitere Informationen erhalten Sie unter Konten registrieren, die bereits vorhanden sind AWS Config Ressourcen und Interagiere mit AWS Control Tower durch AWS CloudShell.
- Wenn das Konto zu einer anderen OU mit einem Verwaltungskonto gehört, einschließlich einer anderen AWS Control Tower-OU, müssen Sie das Konto in der aktuellen OU kündigen, bevor es einer anderen OU beitreten kann. Bestehende Ressourcen müssen in der ursprünglichen Organisationseinheit entfernt werden. Andernfalls schlägt die Anmeldung fehl.

- Die Kontobereitstellung und Registrierung schlägt fehl, wenn die SCPs Ihrer Ziel-OU es Ihnen nicht ermöglichen, alle für dieses Konto erforderlichen Ressourcen zu erstellen. Beispielsweise kann ein SCP in Ihrer Ziel-OU die Erstellung von Ressourcen ohne bestimmte Stichwörter blockieren. In diesem Fall schlägt die Kontobereitstellung oder Registrierung fehl, da AWS Control Tower das Tagging von Ressourcen nicht unterstützt. Wenn Sie Hilfe benötigen, wenden Sie sich an Ihren Kundenbetreuer oder. Support

Weitere Informationen darüber, wie AWS Control Tower mit Rollen arbeitet, wenn Sie neue Konten erstellen oder bestehende Konten registrieren, finden Sie unter Rollen und Konten.

> **Tip**
>
> Wenn Sie nicht bestätigen können, dass eine bestehende Organisationseinheit die Registrierungsvoraussetzungen AWS-Konto erfüllt, können Sie eine Registrierungs-OU einrichten und das Konto bei dieser OU registrieren. Nach erfolgreicher Registrierung können Sie das Konto in die gewünschte Organisationseinheit verschieben. Wenn die Registrierung fehlschlägt, sind keine anderen Konten oder Organisationseinheiten von dem Fehler betroffen.

Wenn Sie Zweifel haben, ob Ihre vorhandenen Konten und deren Konfigurationen mit AWS Control Tower kompatibel sind, können Sie die im folgenden Abschnitt empfohlene Vorgehensweise befolgen.

Empfohlen: Sie können ein zweistufiges Konzept für die Kontoregistrierung einrichten

- Verwenden Sie zunächst ein AWS Config Konformitätspaket, um zu evaluieren, wie sich einige Kontrollen des AWS Control Tower auf Ihre Konten auswirken könnten. Informationen dazu, wie sich die Registrierung bei AWS Control Tower auf Ihre Konten auswirken kann, finden Sie unter Erweitern Sie die AWS Control Tower-Governance mithilfe von AWS Config Conformance Packs.
- Anschließend können Sie das Konto anmelden. Wenn die Compliance-Ergebnisse zufriedenstellend sind, ist der Migrationspfad einfacher, da Sie das Konto ohne unerwartete Folgen anmelden können.
- Wenn Sie sich nach Abschluss Ihrer Bewertung dazu entschließen, eine AWS Control Tower-Landezone einzurichten, müssen Sie möglicherweise den AWS Config Bereitstellungskanal und den Konfigurationsrekorder entfernen, die für Ihre Bewertung erstellt wurden. Dann können Sie den AWS Control Tower erfolgreich einrichten.

> **Note**
>
> Das Conformance Pack funktioniert auch in Situationen, in denen sich die Konten in Organisationseinheiten befinden, die von AWS Control Tower registriert wurden, die Workloads jedoch in AWS Regionen ausgeführt werden, in denen AWS Control Tower nicht unterstützt wird. Sie können das Conformance Pack verwenden, um Ressourcen in Konten zu verwalten, die in Regionen existieren, in denen der AWS Control Tower nicht eingesetzt wird.

Wenn das Konto die Voraussetzungen nicht erfüllt

Denken Sie daran, dass Konten, die für die Registrierung bei AWS Control Tower Governance in Frage kommen, als Voraussetzung derselben Gesamtorganisation angehören müssen. Um diese Voraussetzung für die Kontoregistrierung zu erfüllen, können Sie die folgenden vorbereitenden Schritte befolgen, um ein Konto in dieselbe Organisation wie AWS Control Tower zu verschieben.

Vorbereitende Schritte zur Einrichtung eines Kontos in dieselbe Organisation wie AWS Control Tower

1. Löschen Sie das Konto aus der bestehenden Organisation. Sie müssen eine separate Zahlungsmethode angeben, wenn Sie diesen Ansatz verwenden.
2. Laden Sie das Konto ein, der AWS Control Tower-Organisation beizutreten. Weitere Informationen finden Sie im AWS Organizations Benutzerhandbuch unter Einen AWS Account einladen, Ihrer Organisation beizutreten.
3. Nehmen Sie die Einladung an. Das Konto wird im Stammverzeichnis der Organisation angezeigt. In diesem Schritt wird das Konto in dieselbe Organisation wie AWS Control Tower verschoben. Außerdem werden SCPs und konsolidierte Fakturierungen eingerichtet.

> **Tip**
>
> Sie können die Einladung für die neue Organisation versenden, bevor das Konto aus der alten Organisation ausscheidet. Die Einladung wird warten, wenn das Konto offiziell aus der bestehenden Organisation ausscheidet.

Schritte zur Erfüllung der verbleibenden Voraussetzungen:

1. Erstellen Sie die erforderliche `AWSControlTowerExecution` Rolle.
2. Löschen Sie die Standard-VPC. (Dieser Teil ist optional. AWS Control Tower ändert Ihre bestehende Standard-VPC nicht.)
3. Löschen oder ändern Sie alle vorhandenen AWS Config Konfigurationsrekorder oder Bereitstellungskanäle über das AWS CLI oder AWS CloudShell. Weitere Informationen finden Sie unter Registrieren Sie Konten bei AWS Config Ressourcen und Konten registrieren, die bereits vorhanden sind AWS Config Ressourcen

Nachdem Sie diese vorbereitenden Schritte abgeschlossen haben, können Sie das Konto bei AWS Control Tower registrieren. Weitere Informationen finden Sie unter Schritte zur manuellen Registrierung eines Kontos. Mit diesem Schritt wird das Konto vollständig von AWS Control Tower verwaltet.

Optionale Schritte, um die Bereitstellung eines Kontos aufzuheben, damit es registriert werden kann und seinen Stack behalten kann

1. Um den angewendeten CloudFormation Stack beizubehalten, löschen Sie die Stack-Instance aus den Stack-Sets und wählen Sie Stacks beibehalten für die Instance.
2. Kündigen Sie das vom Konto bereitgestellte Produkt in AWS Service Catalog Account Factory. (In diesem Schritt wird nur das bereitgestellte Produkt aus dem AWS Control Tower entfernt. Das Konto wird dadurch nicht gelöscht.)
3. Richten Sie das Konto mit den erforderlichen Rechnungsdetails ein, wie es für jedes Konto erforderlich ist, das keiner Organisation angehört. Entfernen Sie dann das Konto aus der Organisation. (Sie tun dies, damit das Konto nicht auf die Gesamtsumme Ihres AWS Organizations Kontingents angerechnet wird.)
4. Bereinigen Sie das Konto, falls noch Ressourcen verfügbar sind, und schließen Sie es dann, indem Sie die Schritte zur Kontoschließung unter befolgenMelden Sie ein Konto ab.
5. Wenn Sie eine gesperrte Organisationseinheit mit definierten Kontrollen haben, können Sie das Konto dorthin verschieben, anstatt Schritt 1 auszuführen.

Fügen Sie die erforderliche IAM-Rolle manuell zu einer vorhandenen hinzu AWS-Konto und registriere es

Wenn Sie Ihre AWS Control Tower-Landing Zone bereits eingerichtet haben, können Sie damit beginnen, die Konten Ihrer Organisation bei einer OU zu registrieren, die bei AWS Control Tower registriert ist. Wenn Sie Ihre Landezone noch nicht eingerichtet haben, folgen Sie den Schritten, die im AWS Control Tower-Benutzerhandbuch unter Erste Schritte, Schritt 2 beschrieben sind. Wenn die Landezone fertig ist, führen Sie die folgenden Schritte aus, um bestehende Konten manuell in die Verwaltung durch den AWS Control Tower zu integrieren.

Lesen Sie unbedingt die Voraussetzungen für die Immatrikulation zuvor in diesem Kapitel erläuterten Hinweise.

Bevor Sie ein Konto bei AWS Control Tower registrieren, müssen Sie AWS Control Tower die Erlaubnis geben, dieses Konto zu verwalten. Dazu fügen Sie eine Rolle hinzu, die vollen Zugriff auf das Konto hat, wie in den folgenden Schritten gezeigt. Diese Schritte müssen für jedes Konto ausgeführt werden, das Sie registrieren.

Für jedes Konto:

Schritt 1: Melden Sie sich mit Administratorzugriff auf das Verwaltungskonto der Organisation an, die derzeit das Konto enthält, das Sie registrieren möchten.

Wenn Sie dieses Konto beispielsweise von erstellt haben AWS Organizations und für die Anmeldung eine kontoübergreifende IAM-Rolle verwenden, können Sie die folgenden Schritte ausführen:

1. Melden Sie sich beim Verwaltungskonto Ihrer Organisation an.
2. Wechseln Sie zu AWS Organizations.
3. Wählen Sie unter Konten das Konto aus, das Sie registrieren möchten, und kopieren Sie dessen Konto-ID.
4. Öffnen Sie das Konto-Dropdown-Menü in der oberen Navigationsleiste und wählen Sie Rolle wechseln.
5. Füllen Sie im Formular „Rolle wechseln“ die folgenden Felder aus:
   - Geben Sie unter Konto die Konto-ID ein, die Sie kopiert haben.
   - Geben Sie unter Rolle den Namen der IAM-Rolle ein, die den kontoübergreifenden Zugriff auf dieses Konto ermöglicht. Der Name dieser Rolle wurde bei der Erstellung des Kontos definiert.

Wenn Sie bei der Erstellung des Kontos keinen Rollennamen angegeben haben, geben Sie den Standardrollennamen ein`OrganizationAccountAccessRole`.

6. Wählen Sie Switch Role.
7. Sie sollten jetzt mit dem Konto AWS-Managementkonsole als Kind angemeldet sein.
8. Wenn Sie fertig sind, bleiben Sie für den nächsten Teil des Verfahrens auf dem Kinderkonto.
9. Notieren Sie sich die Verwaltungskonto-ID, da Sie sie im nächsten Schritt eingeben müssen.

Schritt 2: Erteilen Sie AWS Control Tower die Erlaubnis, das Konto zu verwalten.

1. Gehe zu IAM.
2. Gehen Sie zu Rollen.
3. Wählen Sie Rolle erstellen aus.
4. Wenn Sie gefragt werden, für welchen Dienst die Rolle bestimmt ist, wählen Sie Benutzerdefinierte Vertrauensrichtlinie.
5. Kopieren Sie das hier abgebildete Codebeispiel und fügen Sie es in das Richtliniendokument ein. Ersetzen Sie die Zeichenfolge *`Management Account ID`* durch die tatsächliche Verwaltungskonto-ID Ihres Verwaltungskontos. Hier ist die Richtlinie zum Einfügen:

   JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:root"
            },
            "Action": "sts:AssumeRole",
            "Condition": {}
        }
    ]
}
```

6. Wenn Sie aufgefordert werden, Richtlinien anzuhängen, wählen Sie AdministratorAccess.
7. Wählen Sie Next:Tags.

8. Möglicherweise wird ein optionaler Bildschirm mit dem Titel Stichwörter hinzufügen angezeigt. Überspringen Sie diesen Bildschirm vorerst, indem Sie Next:Review
9. Geben Sie auf dem Bildschirm „Überprüfen“ im Feld „Rollenname“ Folgendes ein`AWSControlTowerExecution`.
10. Geben Sie eine kurze Beschreibung in das Feld Beschreibung ein, z. B. Erlaubt vollen Kontozugriff für die Registrierung.
11. Wählen Sie Rolle erstellen aus.

Schritt 3: Registrieren Sie das Konto, indem Sie es in eine registrierte Organisationseinheit verschieben, und überprüfen Sie die Registrierung.

Nachdem Sie die erforderlichen Berechtigungen eingerichtet haben, indem Sie die Rolle erstellt haben, gehen Sie wie folgt vor, um das Konto zu registrieren und die Registrierung zu überprüfen.

1. Melden Sie sich erneut als Admin an und gehen Sie zu AWS Control Tower.
2. Registriere das Konto.
   - Wählen Sie auf der Organisationsseite in AWS Control Tower Ihr Konto aus und wählen Sie dann im Dropdownmenü Aktionen oben rechts die Option Registrieren aus.
   - Folgen Sie den Schritten zur Registrierung eines einzelnen Kontos, wie auf der Seite gezeigt. Schritte zur manuellen Registrierung eines Kontos
3. Überprüfen Sie die Registrierung.
   - Wählen Sie im AWS Control Tower im linken Navigationsbereich Organization aus.
   - Suchen Sie nach dem Konto, das Sie kürzlich registriert haben. Im Anfangsstatus wird der Status „Registrierung“ angezeigt.
   - Wenn sich der Status in Aktiviert ändert, war die Übertragung erfolgreich.

Um diesen Vorgang fortzusetzen, melden Sie sich bei jedem Konto in Ihrer Organisation an, das Sie bei AWS Control Tower registrieren möchten. Wiederholen Sie die erforderlichen Schritte und die Registrierungsschritte für jedes Konto.

Beispiel für das Hinzufügen der Rolle **`AWSControlTowerExecution`**

Die folgende YAML-Vorlage kann Ihnen dabei helfen, die erforderliche Rolle in einem Konto zu erstellen, damit sie programmgesteuert registriert werden kann.

```
AWSTemplateFormatVersion: 2010-09-09
Description: Configure the AWSControlTowerExecution role to enable use of your
  account as a target account in AWS CloudFormation StackSets.
Parameters:
  AdministratorAccountId:
    Type: String
    Description: AWS Account Id of the administrator account (the account in which
      StackSets will be created).
    MaxLength: 12
    MinLength: 12
Resources:
  ExecutionRole:
    Type: AWS::IAM::Role
    Properties:
      RoleName: AWSControlTowerExecution
      AssumeRolePolicyDocument:
        Version: 2012-10-17
        Statement:
          - Effect: Allow
            Principal:
              AWS:
                - !Ref AdministratorAccountId
            Action:
              - sts:AssumeRole
      Path: /
      ManagedPolicyArns:
        - !Sub arn:${AWS::Partition}:iam::aws:policy/AdministratorAccess
```

Konten registrieren, die bereits vorhanden sind AWS Config Ressourcen

In diesem Thema erfahren Sie Schritt für Schritt, wie Sie Konten registrieren, für die bereits Ressourcen vorhanden sind. AWS Config Beispiele dafür, wie Sie Ihre vorhandenen Ressourcen überprüfen können, finden Sie unterRegistrieren Sie Konten bei AWS Config Ressourcen.

Beispiele für AWS Config Ressourcen

Hier sind einige Arten von AWS Config Ressourcen, über die Ihr Konto möglicherweise bereits verfügt. Diese Ressourcen müssen möglicherweise geändert werden, damit Sie Ihr Konto bei AWS Control Tower registrieren können.

- AWS Config Rekorder
- AWS Config Lieferkanal
- AWS Config Autorisierung der Aggregation

Einschränkungen

- Das Registrierungskonto mit vorhandener AWS Config-Ressource wird für Verwaltungskonten oder Serviceintegrationskonten, die in der landing zone konfiguriert sind, nicht unterstützt.
- Das Konto kann nur mithilfe des Workflows zur Registrierung oder erneuten Registrierung der Organisationseinheit registriert werden, der das aktiviert. `AWSControlTowerBaseline` Das Konto kann nicht registriert werden, indem das aktiviert oder zurückgesetzt wird. `ConfigBaseline`
- Ein Konto mit vorhandener AWS Config-Ressource wird von nicht unterstütztKonten mit automatischer Registrierung verschieben und registrieren.
- Wenn die Ressourcen geändert werden und zu Abweichungen auf dem Konto führen, aktualisiert AWS Control Tower die Ressourcen nicht.
- AWS Config Ressourcen in Regionen, die nicht von AWS Control Tower verwaltet werden, werden nicht geändert.

Annahmen

- Sie haben eine AWS Control Tower Tower-Landezone bereitgestellt.
- Ihr Konto ist noch nicht bei AWS Control Tower registriert.
- Ihr Konto verfügt über mindestens eine bereits vorhandene AWS Config Ressource in mindestens einer der Regionen, die von AWS Control Tower verwaltet werden.
- Ihr Konto unterliegt keiner abweichenden Unternehmensführung.

> **Note**
>
> Wenn Sie versuchen, ein Konto mit vorhandenen Config-Ressourcen zu registrieren, ohne dass das Konto der Zulassungsliste hinzugefügt wurde, schlägt die Registrierung fehl. Wenn Sie anschließend versuchen, dasselbe Konto zur Zulassungsliste hinzuzufügen, kann AWS Control Tower nicht überprüfen, ob das Konto korrekt bereitgestellt wurde. Sie müssen die Bereitstellung des Kontos von AWS Control Tower aufheben, bevor Sie die Zulassungsliste

anfordern und dann registrieren können. Wenn Sie das Konto nur auf eine andere AWS Control Tower Tower-Organisationseinheit verschieben, führt dies zu einer Drift in der Unternehmensführung, wodurch auch verhindert wird, dass das Konto zur Zulassungsliste hinzugefügt wird.

Einen Blog, der einen automatisierten Ansatz zur Registrierung von Konten mit vorhandenen AWS Config Ressourcen beschreibt, finden Sie unter Automatisieren der Registrierung von Konten mit vorhandenen AWS Config Ressourcen in AWS Control Tower.

Dieser Prozess besteht aus fünf Hauptschritten.

1. Fügen Sie die Konten zur Zulassungsliste von AWS Control Tower hinzu.
2. Erstellen Sie eine neue IAM-Rolle im Konto.
3. Ändern Sie bereits vorhandene Ressourcen AWS Config .
4. Erstellen Sie AWS Config Ressourcen in AWS Regionen, in denen sie nicht existieren.
5. Registrieren Sie das Konto bei AWS Control Tower.

Bevor Sie fortfahren, sollten Sie die folgenden Erwartungen in Bezug auf diesen Prozess berücksichtigen.

- AWS Control Tower erstellt keine AWS Config Ressourcen in diesem Konto.
- Nach der Registrierung schützen AWS Control Tower Controls automatisch die von Ihnen erstellten AWS Config Ressourcen, einschließlich der neuen IAM-Rolle.
- Wenn nach der Registrierung Änderungen an den AWS Config Ressourcen vorgenommen werden, müssen diese Ressourcen aktualisiert werden, damit sie mit den AWS Control Tower Tower-Einstellungen übereinstimmen, bevor Sie das Konto erneut registrieren können.

Schritt 1: Wenden Sie sich an den Support, um Konten zur Zulassungsliste hinzuzufügen

Fügen Sie diesen Satz in die Betreffzeile Ihres Tickets ein:

Konten mit vorhandenen AWS Config Ressourcen bei AWS Control Tower registrieren

Geben Sie die folgenden Details in den Hauptteil Ihres Tickets ein:

- Kontonummer der Verwaltung
- Kontonummern von Mitgliedskonten, für die bereits AWS Config Ressourcen vorhanden sind. Sie können eine Support-Anfrage für alle Konten erstellen, die Sie registrieren möchten.
- Ihre gewählte Heimatregion für die Einrichtung von AWS Control Tower

> **Note**
>
> Die erforderliche Zeit, um Ihr Konto zur Zulassungsliste hinzuzufügen, beträgt 2 Werktage.

Schritt 2: Erstellen Sie eine neue IAM-Rolle im Mitgliedskonto

1. Öffnen Sie die CloudFormation Konsole für das Mitgliedskonto.
2. Erstellen Sie einen neuen Stack mit der folgenden Vorlage

```
AWSTemplateFormatVersion: 2010-09-09
Description: Configure AWS Config

Resources:
  CustomerCreatedConfigRecorderRole:
    Type: AWS::IAM::Role
    Properties:
      RoleName: aws-controltower-ConfigRecorderRole-customer-created
      AssumeRolePolicyDocument:
        Version: 2012-10-17
        Statement:
          - Effect: Allow
            Principal:
              Service:
                - config.amazonaws.com
            Action:
              - sts:AssumeRole
      Path: /
      ManagedPolicyArns:
        - arn:aws:iam::aws:policy/service-role/AWS_ConfigRole
        - arn:aws:iam::aws:policy/ReadOnlyAccess
```

3. Geben Sie den Namen für den Stack an als CustomerCreatedConfigRecorderRoleForControlTower
4. Erstellen Sie den Stack.

> **Note**
>
> Alle SCPs, die Sie erstellen, sollten eine `aws-controltower-ConfigRecorderRole*` Rolle ausschließen. Ändern Sie nicht die Berechtigungen, die die Fähigkeit von AWS Config Regeln zur Durchführung von Bewertungen einschränken.
> Folgen Sie diesen Richtlinien, damit Sie keine Benachrichtigung erhalten, `AccessDeniedException` wenn Sie SCPs haben, die den Aufruf `aws-controltower-ConfigRecorderRole*` von Config blockieren.

Schritt 3: Identifizieren Sie AWS Regionen mit bereits vorhandenen Ressourcen

Identifizieren und notieren Sie für jede regulierte Region (von AWS Control Tower verwaltet) im Konto die Regionen, in denen mindestens einer der oben aufgeführten AWS Config Ressourcenbeispieltypen vorhanden ist.

Schritt 4: Identifizieren Sie AWS Regionen ohne AWS Config Ressourcen

Identifizieren und notieren Sie für jede regulierte Region (von AWS Control Tower verwaltet) im Konto die Regionen, in denen es keine AWS Config Ressourcen der zuvor gezeigten Beispieltypen gibt.

Schritt 5: Ändern Sie die vorhandenen Ressourcen in jeder AWS Region

Für diesen Schritt werden die folgenden Informationen zu Ihrem AWS Control Tower Tower-Setup benötigt.

- `AUDIT_ACCOUNT`— die ID des AWS Config-Serviceintegrationskontos (früher bekannt als Audit-Konto)
- `CONFIG_BUCKET`— der AWS S3-Bucket, für den AWS Config Konfigurations-Snapshots und Konfigurationsverlaufsdateien bereitstellt. Suchen und bestätigen Sie, dass der AWS S3-Bucket vorhanden ist, bevor Sie mit den nächsten Schritten fortfahren.

  - Für landing zone Version 3.3 oder niedriger hat der AWS S3-Bucket einen Namen`aws-controltower-logs-LOGGING_ACCOUNT-HOME_REGION`, der sich im Logging-Konto befindet.
  - Bei landing zone Zone-Version 4.0 oder höher ist der AWS S3-Bucket benannt `aws-controltower-config-logs-AUDIT_ACCOUNT-<SUFFIX_STRING>` und befindet sich im AWS Config-Serviceintegrationskonto (früher bekannt als Audit-Konto).
- `IAM_ROLE_ARN`— die in Schritt 2 erstellte IAM-Rolle ARN
- `ORGANIZATION_ID`— die Organisations-ID für das Verwaltungskonto
- `MEMBER_ACCOUNT_NUMBER`- das Mitgliedskonto, das geändert wird
- `HOME_REGION`— die Heimatregion für die Einrichtung von AWS Control Tower.

Ändern Sie jede vorhandene Ressource, indem Sie die Anweisungen in den nachfolgenden Abschnitten 5a bis 5c befolgen.

Schritt 5a. AWS Config Ressourcen für Rekorder

Pro AWS Region kann nur ein AWS Config Rekorder existieren. Falls einer vorhanden ist, ändern Sie die Einstellungen wie gezeigt. Ersetzen Sie den Artikel `GLOBAL_RESOURCE_RECORDING` in Ihrer Heimatregion durch true. Ersetzen Sie das Element in anderen Regionen, in denen ein AWS Config Rekorder vorhanden ist, durch „falsch“.

- Name: NICHT ÄNDERN
- RoleARN: `IAM_ROLE_ARN`
  - RecordingGroup:
  - AllSupported: wahr
  - IncludeGlobalResourceTypes: `GLOBAL_RESOURCE_RECORDING`
  - ResourceTypes: Leer

Diese Änderung kann über die AWS CLI mit dem folgenden Befehl vorgenommen werden. Ersetzen Sie die Zeichenfolge `RECORDER_NAME` durch den vorhandenen AWS Config Rekordernamen.

```
aws configservice put-configuration-recorder --configuration-recorder
  name=RECORDER_NAME,roleARN=arn:aws:iam::MEMBER_ACCOUNT_NUMBER:role/
aws-controltower-ConfigRecorderRole-customer-created --recording-group
```

```
 allSupported=true,includeGlobalResourceTypes=GLOBAL_RESOURCE_RECORDING --
region CURRENT_REGION
```

Schritt 5b. Modifizieren Sie AWS Config Ressourcen für den Lieferkanal

Pro Region kann nur ein AWS Config Lieferkanal existieren. Falls ein anderer vorhanden ist, ändern Sie die Einstellungen wie gezeigt.

- Name: NICHT ÄNDERN
- ConfigSnapshotDeliveryProperties: TwentyFour _Stunden
- S3BucketName:*CONFIG_BUCKET*
- S3KeyPrefix: *ORGANIZATION_ID*
- SnsTopicARN: Der SNS-Themen-ARN aus dem Prüfkonto mit dem folgenden Format:

  `arn:aws:sns:CURRENT_REGION:AUDIT_ACCOUNT:aws-controltower-AllConfigNotifications`

Diese Änderung kann über die AWS CLI mit dem folgenden Befehl vorgenommen werden. Ersetzen Sie die Zeichenfolge *DELIVERY_CHANNEL_NAME* durch den vorhandenen AWS Config Rekordernamen.

```
aws configservice put-delivery-channel --delivery-channel
 name=DELIVERY_CHANNEL_NAME,s3BucketName=CONFIG_BUCKET,s3KeyPrefix="ORGANIZATION_ID",configSnap
controltower-AllConfigNotifications --region CURRENT_REGION
```

Schritt 5c. Modifizieren Sie AWS Config Ressourcen für die Aggregation und Autorisierung

> **Note**
>
> Dieser Schritt ist für landing zone Version 4.0 oder höher nicht erforderlich.

Pro Region können mehrere Aggregationsautorisierungen existieren. AWS Control Tower erfordert eine Aggregationsautorisierung, die das Auditkonto als autorisiertes Konto angibt und die Heimatregion für AWS Control Tower als autorisierte Region hat. Falls es nicht existiert, erstellen Sie ein neues mit den folgenden Einstellungen:

- AuthorizedAccountId: Die Audit-Konto-ID
- AuthorizedAwsRegion: Die Heimatregion für das AWS Control Tower Tower-Setup

Diese Änderung kann über die AWS CLI mit dem folgenden Befehl vorgenommen werden:

```
aws configservice put-aggregation-authorization --authorized-account-
id AUDIT_ACCOUNT_ID --authorized-aws-region HOME_REGION --region
CURRENT_REGION
```

Schritt 6: Ressourcen dort erstellen, wo sie nicht existieren, in Regionen, die von AWS Control Tower verwaltet werden

Überarbeiten Sie die CloudFormation Vorlage, sodass der IncludeGlobalResourcesTypesParameter in Ihrer Heimatregion den Wert hat`GLOBAL_RESOURCE_RECORDING`, wie im folgenden Beispiel gezeigt. Aktualisieren Sie außerdem die erforderlichen Felder in der Vorlage, wie in diesem Abschnitt beschrieben.

Ersetzen Sie den Artikel `GLOBAL_RESOURCE_RECORDING` in Ihrer Heimatregion durch true. Ersetzen Sie den Eintrag durch „Falsch“ für andere Regionen, in denen kein AWS Config Rekorder vorhanden ist.

1. Navigieren Sie zur CloudFormation Konsole des Verwaltungskontos.
2. Erstellen Sie ein neues StackSet mit dem Namen CustomerCreatedConfigResourcesForControlTower.
3. Kopieren und aktualisieren Sie die folgende Vorlage:

> **Note**
>
> Die `CustomerCreatedAggregationAuthorization` Ressource in der Vorlage ist für landing zone Version 4.0 oder höher nicht erforderlich.

```
AWSTemplateFormatVersion: 2010-09-09
Description: Configure AWS Config
Resources:
  CustomerCreatedConfigRecorder:
    Type: AWS::Config::ConfigurationRecorder
    Properties:
      Name: aws-controltower-BaselineConfigRecorder-customer-created
      RoleARN: !Sub arn:aws:iam::${AWS::AccountId}:role/aws-controltower-
ConfigRecorderRole-customer-created
      RecordingGroup:
        AllSupported: true
        IncludeGlobalResourceTypes: GLOBAL_RESOURCE_RECORDING
        ResourceTypes: []
  CustomerCreatedConfigDeliveryChannel:
    Type: AWS::Config::DeliveryChannel
    Properties:
      Name: aws-controltower-BaselineConfigDeliveryChannel-customer-created
      ConfigSnapshotDeliveryProperties:
        DeliveryFrequency: TwentyFour_Hours
      S3BucketName: CONFIG_BUCKET
      S3KeyPrefix: ORGANIZATION_ID
      SnsTopicARN: !Sub arn:aws:sns:${AWS::Region}:AUDIT_ACCOUNT:aws-controltower-
AllConfigNotifications
  CustomerCreatedAggregationAuthorization:
    Type: "AWS::Config::AggregationAuthorization"
    Properties:
      AuthorizedAccountId: AUDIT_ACCOUNT
      AuthorizedAwsRegion: HOME_REGION
```

Aktualisieren Sie die Vorlage mit den erforderlichen Feldern:

a. Ersetzen Sie in dem S3BucketNameFeld die *CONFIG_BUCKET*

b. Ersetzen Sie in dem S3KeyPrefixFeld den *ORGANIZATION_ID*

c. Ersetzen SnsTopicSie im ARN-Feld den *AUDIT_ACCOUNT*

d. Ersetzen Sie in dem AuthorizedAccountIdFeld den *AUDIT_ACCOUNT*

e. Ersetzen Sie in dem AuthorizedAwsRegionFeld den *HOME_REGION*

4. Fügen Sie während der Bereitstellung auf der CloudFormation Konsole die Mitgliedskontonummer hinzu.
5. Fügen Sie die AWS Regionen hinzu, die in Schritt 4 identifiziert wurden.

6. Stellen Sie das Stack-Set bereit.

Schritt 7: Registrieren Sie die Organisationseinheit bei AWS Control Tower

Registrieren Sie die Organisationseinheit im AWS Control Tower Tower-Dashboard.

> **Note**
>
> Der Workflow zur Kontoregistrierung wird für diese Aufgabe nicht erfolgreich sein. Sie müssen „Organisationseinheit registrieren“ oder Re-register „Organisationseinheit registrieren“ wählen.

Bereitstellung und Verwaltung von Konten mit Account Factory

> **Note**
>
> Die Bereitstellung, Aktualisierung und Anpassung eines einzelnen Kontos muss auf eine Organisationseinheit (OU) abzielen, die AWSControlTowerBaseline aktiviert ist. Wenn für eine Organisationseinheit diese Option nicht AWSControlTowerBaseline aktiviert ist, können Sie die automatische Kontoregistrierung aktivieren oder zur Kontoregistrierung ResetEnabledBaseline beliebige ResetEnabledControl APIs auf EnabledBaselines und EnabledControls auf dieser Organisationseinheit verwenden. Einzelheiten finden Sie unter:. AWSControlTowerBaseline Basistypen, die auf OU-Ebene gelten

Dieses Kapitel enthält eine Übersicht und Verfahren für die Bereitstellung neuer Mitgliedskonten in einer AWS Control Tower-Landezone mit Account Factory.

Berechtigungen für die Konfiguration und Bereitstellung von Konten

Die AWS Control Tower Account Factory ermöglicht es Cloud-Administratoren und Benutzern AWS IAM Identity Center , Konten in Ihrer Landing Zone bereitzustellen. Standardmäßig müssen IAM Identity Center-Benutzer, die Konten bereitstellen, der `AWSAccountFactory` Gruppe oder der Verwaltungsgruppe angehören.

> **Note**
>
> Seien Sie vorsichtig, wenn Sie vom Verwaltungskonto aus arbeiten, wie Sie es tun würden, wenn Sie jedes Konto verwenden, das über Berechtigungen in Ihrer gesamten Organisation verfügt.

Das AWS Control Tower-Verwaltungskonto hat eine Vertrauensbeziehung mit der `AWSControlTowerExecution` Rolle, was die Kontoeinrichtung vom Verwaltungskonto aus ermöglicht, einschließlich einiger automatisierter Kontoeinrichtungen. Weitere Informationen zur `AWSControlTowerExecution` Rolle finden Sie unter Rollen und Konten.

> **Note**
>
> Um ein bestehendes AWS-Konto Konto bei AWS Control Tower zu registrieren, muss für dieses Konto die `AWSControlTowerExecution` Rolle aktiviert sein. Weitere Informationen zum Registrieren eines vorhandenen Kontos finden Sie unter Über das Registrieren vorhandener Konten.

Weitere Informationen zu Berechtigungen finden Sie unter Für die Bereitstellung von Konten sind Berechtigungen erforderlich.

Überlegungen zur Verwaltung von Konten in Account Factory

Sie können Konten, die Sie über Account Factory erstellen und bereitstellen, aktualisieren, abmelden und schließen. Sie können Konten recyceln, indem Sie die Benutzerparameter in den Konten aktualisieren, die Sie wiederverwenden möchten. Sie können auch die Organisationseinheit (OU) eines Kontos ändern.

> **Note**
>
> Wenn Sie bei der Aktualisierung eines bereitgestellten Produkts, das mit einem Konto verknüpft ist, das Account Factory verkauft, eine neue Benutzer-E-Mail-Adresse angeben AWS IAM Identity Center, erstellt AWS Control Tower einen neuen Benutzer im IAM Identity Center. Das zuvor erstellte Konto wird nicht entfernt. Informationen zum Entfernen der E-Mail-Adresse des vorherigen IAM Identity Center-Benutzers aus dem IAM Identity Center finden Sie unter Benutzer deaktivieren.

Konten mit AWS Control Tower aktualisieren und verschieben

Der einfachste Weg, ein registriertes Konto zu aktualisieren, ist über die AWS Control Tower-Konsole. Individuelle Kontoaktualisierungen sind nützlich, um Abweichungen zu beheben, z. B. Mitgliedskonto wurde verschoben Kontoaktualisierungen sind auch im Rahmen einer vollständigen Aktualisierung der Landezone erforderlich.

Aktualisiere das Konto in der Konsole

Um ein Konto in der AWS Control Tower-Konsole zu aktualisieren

1. Wenn Sie bei AWS Control Tower angemeldet sind, navigieren Sie zur Seite Organisation.
2. Wählen Sie in der Liste der Organisationseinheiten und Konten den Namen des Kontos aus, das Sie aktualisieren möchten. Konten, für die eine Aktualisierung verfügbar ist, haben den Status Update verfügbar.
3. Als Nächstes wird die Seite mit den Kontodetails für das von Ihnen gewählte Konto angezeigt.
4. Wählen Sie oben rechts Konto aktualisieren aus.

Wenn Sie ein Konto von einer Organisationseinheit (OU) in eine andere verschieben, denken Sie daran, dass sich die von der neuen OU angewendeten Steuerelemente von den Steuerelementen in der vorherigen OU unterscheiden können. Stellen Sie sicher, dass die Steuerelemente in der neuen Organisationseinheit Ihren Richtlinienanforderungen für das Konto entsprechen.

AWS Control Tower-Konten werden unterschiedlich geändert, je nachdem, ob Sie sich für die automatische Registrierung von Konten entschieden haben oder nicht. Weitere Informationen zur automatischen Registrierung finden Sie unter. Konfigurieren Sie optional die automatische Registrierung für Konten

Steuern Sie das Verhalten, wenn Konten zwischen Konten verschoben werden Organisationseinheiten, bei denen die automatische Registrierung aktiviert ist

Wenn Sie ein Konto in eine neue Organisationseinheit verschieben, wendet AWS Control Tower die aktivierten Basislinien und Kontrollen der Organisationseinheit auf das Konto an. Kontrollen und Baselines aus der vorherigen OU werden entfernt. Wenn Sie ein Konto außerhalb einer registrierten Organisationseinheit verschieben, entfernt AWS Control Tower alle bereitgestellten Baselines und Kontrollen.

Steuern Sie das Verhalten, wenn Konten zwischen Konten verschoben werden

Organisationseinheiten, ohne automatische Registrierung

Wenn Sie ein Konto zwischen Organisationseinheiten verschieben, werden die Steuerelemente für die Ziel-OU auf
Konto. Die Steuerelemente, die von der früheren Organisationseinheit für das Konto galten, sind es jedoch nicht
entfernt. Das genaue Verhalten der Steuerelemente ist spezifisch für die Implementierung der Steuerelemente, die auf der vorherigen Organisationseinheit und der Ziel-OU aktiv sind.

- Für Steuerelemente, die mit AWS Config Regeln implementiert wurden: Die Steuerelemente der vorherigen Organisationseinheit
  werden nicht entfernt. Diese Steuerungen müssen manuell entfernt werden.
- Für Steuerungen, die mit SCPs implementiert wurden: Die SCP-based Steuerelemente aus der vorherigen OU sind
  entfernt. Die SCP-based Steuerungen für die Ziel-OU treten für dieses Konto in Kraft.
- Für Steuerelemente, die mit CloudFormation Hooks implementiert sind: Dieses Verhalten hängt vom Status der Steuerelemente in der neuen Organisationseinheit ab.
  - Wenn in der Ziel-OU keine Hook-basierten Steuerelemente aktiv sind: Die alte
    Die Steuerelemente für das verschobene Konto bleiben aktiv, sofern Sie sie nicht entfernen manuell.
  - Wenn in der Ziel-OU Hook-Steuerelemente aktiv sind: Die alten Steuerelemente sind entfernt und die Steuerelemente in der Ziel-OU werden auf die angewendet
    Konto.

E-Mail-Adresse eines registrierten Kontos ändern

Gehen Sie wie in diesem Abschnitt beschrieben vor, um die E-Mail-Adresse eines registrierten AWS Control Tower-Kontos zu ändern.

> **Ändern der E-Mail-Adressen des Verwaltungskontos**
>
> Um die E-Mail-Adresse eines AWS Verwaltungskontos zu ändern, melden Sie sich als Root-Benutzer mit Administratorrechten an.

Ändern Sie die E-Mail-Adresse mit AWS Organizations

1. Anweisungen zum Aktualisieren der E-Mail-Adresse des Root-Benutzers finden Sie im Referenzhandbuch zur Kontoverwaltung unter Aktualisieren der E-Mail-Adresse des Root-Benutzers für ein AWS Mitgliedskonto.
2. Nachdem Sie die E-Mail-Adresse aktualisiert haben, aktualisieren Sie das Konto im AWS Control Tower. Dieses Update verknüpft die neue E-Mail-Adresse mit dem Konto in AWS Control Tower. Wenn Sie das Konto über das von Service Catalog bereitgestellte Produkt aktualisieren, geben Sie die alte E-Mail-Adresse als Wert für den `AccountEmail` Parameter an.

Ändern Sie die E-Mail-Adresse mithilfe der Root-Benutzeranmeldedaten

1. Stellen Sie das Root-Benutzerkennwort für das Konto wieder her. Anweisungen zum Wiederherstellen eines verlorenen Passworts finden Sie unter Wie stelle ich ein verlorenes oder vergessenes AWS Passwort wieder her?
2. Melden Sie sich mit dem Root-Benutzerkennwort beim Konto an.
3. Ändern Sie die E-Mail-Adresse wie bei jeder anderen und warten Sie AWS-Konto, bis die Änderung wirksam wird AWS Organizations. Es kann zu einer Verzögerung kommen, bis die Aktualisierung der Änderung der E-Mail-Adresse abgeschlossen ist.
4. Nachdem Sie die E-Mail-Adresse aktualisiert haben, aktualisieren Sie das Konto im AWS Control Tower. Dieses Update verknüpft die neue E-Mail-Adresse mit dem Konto in AWS Control Tower. Wenn Sie das Konto über das von Service Catalog bereitgestellte Produkt aktualisieren, geben Sie die alte E-Mail-Adresse als Wert für den `AccountEmail` Parameter an.

Ändern Sie den Namen eines registrierten Kontos

Folgen Sie den Anweisungen in diesem Abschnitt, um den Namen eines registrierten AWS Control Tower-Kontos zu ändern.

> **Note**
>
> Um den Namen eines AWS Administratorkontos zu ändern, müssen Sie über Administratorrechte verfügen und als Root-Benutzer des Kontos angemeldet sein.

Um den Namen eines von AWS Control Tower erstellten Kontos zu ändern, verwenden Sie AWS Organizations Konsole oder APIs

- Folgen Sie den Anweisungen im Referenzhandbuch zur AWS Kontoverwaltung.

Alternative Methode, um den Namen eines von AWS Control Tower erstellten Kontos zu ändern

1. Stellen Sie das Root-Passwort für das Konto wieder her. Sie können die in diesem Artikel beschriebenen Schritte befolgen. Wie stelle ich ein verlorenes oder vergessenes AWS Passwort wieder her?
2. Loggen Sie sich mit dem Root-Passwort in das Konto ein.
3. Navigieren Sie in der AWS Billing Konsole zur Seite mit den Kontoeinstellungen.
4. Ändern Sie den Namen in den Kontoeinstellungen wie bei jedem anderen Namen AWS-Konto.
5. Der AWS Control Tower aktualisiert sich automatisch, um die Namensänderung widerzuspiegeln. Dieses Update wird sich nicht auf das bereitgestellte Produkt in AWS Service Catalog auswirken.

Konfigurieren Sie Account Factory mit den Amazon Virtual Private Cloud-Einstellungen

Mit Account Factory können Sie vorab genehmigte Basispläne und Konfigurationsoptionen für Konten in Ihrer Organisation erstellen. Sie können die Konfiguration und Bereitstellung neuer Konten in AWS Service Catalog vornehmen.

Auf der Account Factory-Seite sehen Sie eine Liste der Organisationseinheiten (OUs) und deren Status in der Zulassungsliste. Standardmäßig werden alle OUs auf die Whitelist gesetzt. Dies bedeutet, dass Konten unter ihnen bereitgestellt werden können. Sie können bestimmte OUs für die Kontobereitstellung über AWS Service Catalog deaktivieren.

Sie können die Amazon VPC-Konfigurationsoptionen einsehen, die Ihren Endbenutzern bei der Bereitstellung neuer Konten zur Verfügung stehen.

Um die Amazon VPC-Einstellungen in Account Factory zu konfigurieren

1. Melden Sie sich als zentraler Cloud-Administrator mit Administratorberechtigungen im Verwaltungskonto bei der AWS Control Tower-Konsole an.
2. Wählen Sie auf der linken Seite des Dashboards Account Factory aus, um zur Account Factory-Netzwerkkonfigurationsseite zu gelangen. Dort werden die Standardnetzwerkeinstellungen

angezeigt. Wählen Sie zum Bearbeiten Bearbeiten aus und sehen Sie sich die bearbeitbare Version Ihrer Account Factory-Netzwerkkonfigurationseinstellungen an.

3. Sie können jedes Feld der Standardeinstellungen nach Bedarf ändern. Wählen Sie die VPC-Konfigurationsoptionen, die Sie für alle neuen Account Factory-Konten einrichten möchten, die Ihre Endbenutzer möglicherweise erstellen, und geben Sie Ihre Einstellungen in die Felder ein.

- Wählen Sie deaktiviert oder aktiviert, um ein öffentliches Subnetz in Amazon VPC zu erstellen. Standardmäßig ist das über das Internet zugängliche Subnetz nicht zulässig.

> **Note**
>
> Wenn Sie in der VPC-Konfiguration von Account Factory einstellen, dass öffentliche Subnetze bei der Bereitstellung eines neuen Kontos aktiviert sind, konfiguriert Account Factory Amazon VPC so, dass ein NAT-Gateway erstellt wird. Seine Nutzung wird Ihnen von Amazon VPC in Rechnung gestellt. Weitere Informationen finden Sie unter VPC Preise.

- Wählen Sie die maximale Anzahl an privaten Subnetzen in Amazon VPC aus der Liste aus. Standardmäßig ist 1 ausgewählt. Die maximal zulässige Anzahl an privaten Subnetzen beträgt 2 pro Verfügbarkeitszone.
- Geben Sie den IP-Adressbereich zum Erstellen von Konto-VPCs an. Der Wert muss das Format eines Classless Inter-Domain Routing(CIDR)-Blocks (der Standard ist z. B. `172.31.0.0/16`) aufweisen. Dieser CIDR-Block stellt den Gesamtbereich der Subnetz-IP-Adressen für die VPC bereit, die Account Factory für Ihr Konto erstellt. Innerhalb Ihrer VPC werden Subnetze automatisch aus dem von Ihnen angegebenen Bereich zugewiesen und haben dieselbe Größe. Standardmäßig überschneiden sich Subnetze in Ihrer VPC nicht. Die IP-Adressbereiche des Subnetzes in den VPCs aller Ihrer bereitgestellten Konten können sich jedoch überschneiden.
- Wählen Sie eine Region oder alle Regionen für das Erstellen einer VPC aus, wenn ein Konto bereitgestellt wird. Standardmäßig sind alle verfügbaren Regionen ausgewählt.
- Wählen Sie in der Liste die Anzahl der Availability Zones aus, für die Subnetze in jeder VPC konfiguriert werden sollen. Die standardmäßige und empfohlene Anzahl ist 3.
- Wählen Sie Speichern.

Sie können diese Konfigurationsoptionen für die Erstellung neuer Konten, die keine VPC enthalten, einrichten. Sehen Sie sich die exemplarische Vorgehensweise an.

Melden Sie ein Konto ab

Wenn Sie ein Konto in Account Factory erstellt oder registriert haben und Sie nicht mehr möchten AWS-Konto, dass das Konto von AWS Control Tower in einer Landing Zone verwaltet wird, können Sie das Konto von der AWS Control Tower-Konsole aus deregistrieren.

Wenn Sie die Registrierung eines AWS Control Tower-Kontos aufheben, werden alle vom AWS Control Tower bereitgestellten Ressourcen entfernt, einschließlich aller Kontrollen und Blueprints. Das Konto wird aus einer beliebigen AWS Control Tower-OU in den Root-Bereich verschoben. Das Konto ist nicht mehr Teil einer registrierten OU und unterliegt nicht mehr den AWS Control Tower SCPs. Sie können das Konto über AWS Organizations schließen.

Um ein registriertes Konto von der AWS Control Tower-Konsole aus abzumelden

1. Öffnen Sie die AWS Control Tower-Konsole in Ihrem Webbrowser unter https://console.aws.amazon.com/controltower
2. Wählen Sie im linken Navigationsbereich Organisation aus.
3. Erweitern Sie auf der Seite „Organisation“ die Organisationseinheit, die das Konto enthält, indem Sie auf die Schaltfläche „+“ neben der Organisationseinheit klicken.
4. Wählen Sie das Konto aus und klicken Sie dann auf Verwaltung aufheben.

> **Note**
>
> Warten Sie, bis der Kontostatus Nicht registriert angezeigt wird.

Wenn Sie das Konto nicht mehr benötigen, schließen Sie es. Weitere Informationen zum Schließen von AWS Konten finden Sie im AWS Billing Benutzerhandbuch unter Konto schließen

> **Heben Sie die Registrierung eines Kontos auf, wenn die automatische Registrierung aktiv ist**
>
> Wenn die Funktion zur automatischen Registrierung auf Ihrer Einstellungsseite aktiv ist, können Sie die Registrierung eines Kontos auch aufheben, indem Sie es in eine Organisationseinheit verschieben, die nicht im AWS Control Tower registriert ist. Alle AWS Control Tower-Ressourcen werden entfernt. Beachten Sie, dass Sie das Konto nicht versehentlich auf diese Weise abmelden. Sie können das Konto jedoch erneut registrieren, indem Sie es an die OU zurückgeben.

Wenn Sie die Registrierung eines benutzerdefinierten Kontos aufheben, entfernt AWS Control Tower die Ressourcen, die die Landing Zone bereitgestellt hat, sowie alle anderen Ressourcen, die AWS Control Tower innerhalb des Kontos erstellt hat. AWS Control Tower entfernt die AWSControlTowerExecution Rolle auch dann, wenn sie manuell hinzugefügt wurde. Das Entfernen dieser Rolle entspricht dem Prinzip der geringsten Rechte, da eine Rolle, die einen Service ausführt, nicht in einem unverwalteten Konto verbleiben sollte.

Nachdem Sie das Konto deregistriert haben, können Sie das Konto über schließen. AWS Organizations

> **Note**
>
> Ein Konto, bei dem die Registrierung aufgehoben wurde, wird nicht geschlossen oder gelöscht. Wenn das Konto deregistriert wurde, hat der IAM Identity Center-Benutzer, den Sie bei der Erstellung des Kontos in Account Factory ausgewählt haben, weiterhin Administratorzugriff auf das Konto. Wenn Sie nicht möchten, dass dieser Benutzer Administratorzugriff hat, müssen Sie diese Einstellung im IAM Identity Center ändern, indem Sie das Konto in Account Factory aktualisieren und die IAM Identity Center-Benutzer-E-Mail-Adresse für das Konto ändern. Weitere Informationen finden Sie unter Konten mit AWS Control Tower aktualisieren und verschieben.

Video-Anleitung

Dieses Video (3:25) beschreibt, wie Sie ein Konto aus dem AWS Control Tower entfernen, Root-Zugriff auf das Konto erhalten und schließlich das schließen. AWS-Konto Sie können ein Konto auch mit einer AWS Organizations API schließen. Wählen Sie zur besseren Ansicht das Symbol in der rechten unteren Ecke des Videos, um es in voller Bildschirmgröße anzuzeigen. Es stehen Untertitel zur Verfügung.

Videoanleitung zur Schließung eines Kontos im AWS Control Tower.

Schließen Sie ein in Account Factory erstelltes Konto

In Account Factory erstellte Konten sind AWS-Konten. Informationen zum Schließen AWS-Konten eines Kontos finden Sie im Referenzhandbuch zur AWS Kontoverwaltung unter Konto schließen .

> **Note**
>
> Das Schließen eines Kontos AWS-Konto ist nicht dasselbe wie das Abmelden eines Kontos bei AWS Control Tower — dies sind separate Aktionen. Sie müssen das Konto abmelden, bevor Sie es schließen.

Schließen Sie ein AWS Control Tower-Mitgliedskonto über AWS Organizations

Sie können Ihre AWS Control Tower-Mitgliedskonten vom Verwaltungskonto Ihrer Organisation aus schließen, ohne dass Sie sich bei jedem Mitgliedskonto einzeln mit Root-Anmeldeinformationen anmelden müssen AWS Organizations. Verwenden Sie dazu Sie können Ihr Verwaltungskonto jedoch nicht auf diese Weise schließen.

Wenn Sie die AWS Organizations CloseAccount API aufrufen oder ein Konto in der AWS Organizations Konsole schließen, ist das Mitgliedskonto wie jedes andere für 90 AWS-Konto Tage isoliert. Das Konto zeigt im AWS Control Tower den Status Gesperrt an und AWS Organizations. Wenn Sie während dieser 90 Tage versuchen, mit dem Konto zu arbeiten, gibt AWS Control Tower eine Fehlermeldung aus.

> **Note**
>
> Wenn eine OU Konten gesperrt hat EnabledControl , schlagen die regionalen Kontrollen am Ziel fehl.

Vor Ablauf der 90 Tage können Sie das Mitgliedskonto wie jedes andere Konto wiederherstellen AWS-Konto. Nach Ablauf dieser 90 Tage werden die Aufzeichnungen des Kontos entfernt.

Wir empfehlen als bewährte Methode, die Registrierung eines Mitgliedskontos aufzuheben, bevor Sie dieses Konto schließen. Wenn Sie ein Mitgliedskonto schließen, ohne es zuvor zu verwalten, zeigt AWS Control Tower den Status des Kontos als Gesperrt, aber auch als Registriert an. Wenn Sie also während dieser 90 Tage versuchen, Re-register die Organisationseinheit des Kontos aufzurufen, gibt AWS Control Tower eine Fehlermeldung aus. Das gesperrte Konto blockiert im Wesentlichen die Aktionen zur erneuten Registrierung, da die Vorabprüfung fehlschlägt. Wenn Sie das Konto aus der OU entfernen, können Sie Re-register die OU zwar wieder verwenden, es AWS kann jedoch zu einem Fehler aufgrund einer fehlenden Zahlungsmethode für das Konto kommen. Um diese Einschränkung zu umgehen, erstellen Sie eine weitere OU und verschieben Sie das Konto in

diese OU, bevor Sie versuchen, sich erneut zu registrieren. Wir empfehlen, diese OU als Suspended OU zu bezeichnen.

> **Note**
>
> Wenn Sie das Konto nicht abmelden, bevor Sie es schließen, müssen Sie das für das Konto bereitgestellte Produkt AWS Service Catalog nach Ablauf dieser 90 Tage löschen.

Weitere Informationen finden Sie in der AWS Organizations Dokumentation zur API. CloseAccount

Überlegungen zu Ressourcen für Account Factory

Wenn ein Konto mit Account Factory bereitgestellt wird, werden die folgenden AWS Ressourcen innerhalb des Kontos erstellt.

AWS Dienst	Ressourcentyp	Ressourcenname
AWS CloudFormation	Stacks	StackSet-AWSControlTowerBP-BASELINE-CLOUDTRAIL-*(Nicht in der Landing Zone-Version 3.0 und höher bereitgestellt) StackSet-AWSControlTowerBP-BASELINE-CLOUDWATCH-* StackSet-AWSControlTowerBP-BASELINE-CONFIG-* StackSet-AWSControlTowerBP-BASELINE-ROLES-* StackSet-AWSControlTowerBP-BASELINE-SERVICE-ROLES-*

AWS Dienst	Ressourcentyp	Ressourcenname
AWS CloudTrail	Trail	aws-controltower-BaselineCloudTrail
AWS Config	Lieferkanal	aws-controltower-BaselineConfigDeliveryChannel
AWS Config	Rekorder	aws-controltower-BaselineConfigRecorder
Amazon CloudWatch	CloudWatch Logs	/aws/lambda/aws-controltower-NotificationForwarder
AWS Identity and Access Management	Rollen	aws-controltower-AdministratorExecutionRole aws-controltower-CloudWatchLogsRole(Nicht in der Landing Zone-Version 3.0 und höher bereitgestellt) aws-controltower-ConfigRecorderRole(Nicht in der Landing Zone-Version 2.8 und höher eingesetzt) aws-controltower-ForwardSnsNotificationRole aws-controltower-ReadOnlyExecutionRole AWSControlTowerExecution
AWS Identity and Access Management	Richtlinien	AWSControlTowerServiceRolePolicy
Amazon Simple Notification Service	Topics	aws-controltower-SecurityNotifications

AWS Dienst	Ressourcentyp	Ressourcenname
AWS Lambda	Anwendungen	StackSet-AWSControlTowerBP-BASELINE-CLOUDWATCH-*
AWS Lambda	Funktionen	aws-controltower-NotificationForwarder
Amazon EventBridge	Regel	AWSControlTowerManagedRule
Amazonas EventBridge	Regel	aws-controltower-ConfigComplianceChangeEventRule

Passen Sie Konten mit Account Factory Customization (AFC) an

> **Note**
>
> Die Bereitstellung, Aktualisierung und Anpassung eines einzelnen Kontos muss auf eine Organisationseinheit (OU) abzielen, die AWSControlTowerBaseline aktiviert ist. Wenn für eine Organisationseinheit diese Option nicht AWSControlTowerBaseline aktiviert ist, können Sie die automatische Kontoregistrierung aktivieren oder zur Kontoregistrierung ResetEnabledBaseline beliebige ResetEnabledControl APIs auf EnabledBaselines und EnabledControls auf dieser Organisationseinheit verwenden. Einzelheiten finden Sie unter:. AWSControlTowerBaseline Basistypen, die auf OU-Ebene gelten

Mit AWS Control Tower können Sie neue und bestehende Ressourcen individuell anpassen AWS-Konten , wenn Sie deren Ressourcen über die AWS Control Tower-Konsole bereitstellen. Nachdem Sie die Account Factory-Anpassung eingerichtet haben, automatisiert AWS Control Tower diesen Prozess für die zukünftige Bereitstellung, sodass Sie keine Pipelines verwalten müssen. Benutzerdefinierte Konten können sofort nach der Bereitstellung der Ressourcen verwendet werden.

Stellen Sie neue Konten mit Blueprints bereit

Ihre benutzerdefinierten Konten werden in der AWS Control Tower Account Factory, über CloudFormation Vorlagen oder mit Terraform bereitgestellt. Sie definieren eine Vorlage, die als

benutzerdefinierter Konto-Blueprint dient. Ihr Blueprint beschreibt die spezifischen Ressourcen und Konfigurationen, die Sie für die Bereitstellung eines Kontos benötigen. Pre-defined Blueprints, die von AWS Partnern erstellt und verwaltet werden, sind ebenfalls verfügbar. Weitere Informationen zu von Partnern verwalteten Blueprints finden Sie in der AWS Service Catalog Bibliothek „Erste Schritte“.

Wenden Sie Blueprints auf bestehende Konten an

Sie können benutzerdefinierte Blueprints auch auf bestehende Konten anwenden, indem Sie die Schritte zur Kontoaktualisierung in der AWS Control Tower-Konsole befolgen. Details hierzu finden Sie unter Aktualisiere das Konto in der Konsole.

Definition: Ihr Hub-Konto

Ihre Konto-Blueprints werden in einem gespeichert AWS-Konto, das für unsere Zwecke als Hub-Konto bezeichnet wird. Blueprints werden in Form eines Service Catalog-Produkts gespeichert. Wir nennen dieses Produkt einen Blueprint, um es von allen anderen Service Catalog-Produkten zu unterscheiden. Weitere Informationen zum Erstellen von Service Catalog-Produkten finden Sie unter Erstellen von Produkten im AWS Service Catalog Administratorhandbuch.

> **Note**
>
> AWS Control Tower enthält proaktive Kontrollen, die die CloudFormation Ressourcen im AWS Control Tower überwachen. Optional können Sie diese Steuerungen in Ihrer Landezone aktivieren. Wenn du proaktive Kontrollen anwendest, wird überprüft, ob die Ressourcen, die du für deine Konten bereitstellen möchtest, den Richtlinien und Verfahren deiner Organisation entsprechen. Weitere Informationen zu proaktiven Kontrollen finden Sie unter Proaktive Kontrollen.

Weitere Informationen zur Arbeit mit AFC finden Sie unter Automatisieren der Kontoanpassung mithilfe der Account Factory-Anpassung in AWS Control Tower.

> **Voraussetzungen**
>
> Bevor Sie mit der Erstellung benutzerdefinierter Konten mit AWS Control Tower Account Factory beginnen, müssen Sie eine AWS Control Tower-Landing Zone-Umgebung bereitstellen und eine Organisationseinheit (OU) bei AWS Control Tower registriert haben, in der Ihre neu erstellten Konten platziert werden.

Vorbereitung der Anpassung

- Benennen Sie ein Hub-Konto: Sie können ein neues Konto erstellen, das als Hub-Konto dient, oder Sie können ein AWS-Konto vorhandenes verwenden. Wir empfehlen dringend, dass Sie das AWS Control Tower-Managementkonto nicht als Ihr Blueprint-Hub-Konto verwenden.
- Fügen Sie die erforderliche Rolle hinzu: Wenn Sie planen, sich bei AWS Control Tower AWS-Konten zu registrieren und sie anzupassen, müssen Sie zuerst die `AWSControlTowerExecution` Rolle zu diesen Konten hinzufügen, wie Sie es für jedes andere Konto tun würden, das Sie bei AWS Control Tower registrieren.
- Partner-Blueprints konfigurieren (optional): Wenn Sie Partner-Blueprints verwenden möchten, für die Marketplace-Abonnementanforderungen gelten, müssen Sie diese von Ihrem AWS Control Tower-Verwaltungskonto aus konfigurieren, bevor Sie die Partner-Blueprints als Blueprints zur werkseitigen Anpassung des Kontos bereitstellen.

Themen

- Für die Anpassung einrichten
- Erstellen Sie ein benutzerdefiniertes Konto anhand eines Blueprints
- Passen Sie Konten bei AFC an, während Sie sie registrieren
- Fügen Sie einem AWS Control Tower-Konto einen Blueprint hinzu
- Aktualisieren Sie einen Blueprint
- Einen Blueprint aus einem Konto entfernen
- Pläne von Partnern
- Überlegungen zu Account Factory-Anpassungen (AFC)
- Im Falle eines Blueprint-Fehlers
- Anpassung Ihres Richtliniendokuments für AFC-Blueprints auf der Grundlage von CloudFormation
- Für die Erstellung eines Terraform-based Service Catalog-Produkts sind zusätzliche Berechtigungen erforderlich
- Übergang zum AWS Service Catalog Externer Produkttyp

Für die Anpassung einrichten

In den nächsten Abschnitten finden Sie Schritte zur Einrichtung von Account Factory für den Anpassungsprozess. Wir empfehlen, dass Sie einen delegierten Administrator für das Hub-Konto einrichten, bevor Sie mit diesen Schritten beginnen.

Zusammenfassung

- Schritt 1. Erstellen Sie die erforderliche Rolle. Erstellen Sie eine IAM-Rolle, die AWS Control Tower den Zugriff auf das (Hub-) Konto gewährt, in dem die Service Catalog-Produkte, auch Blueprints genannt, gespeichert sind.
- Schritt 2. Erstellen Sie das Produkt AWS Service Catalog . Erstellen Sie das AWS Service Catalog Produkt (auch als „Blueprint-Produkt“ bezeichnet), das Sie für das Baselining des benutzerdefinierten Kontos benötigen.
- Schritt 3. Überprüfen Sie Ihren benutzerdefinierten Blueprint. Untersuchen Sie das AWS Service Catalog Produkt (Blueprint), das Sie erstellt haben.
- Schritt 4. Rufen Sie Ihren Blueprint auf, um ein benutzerdefiniertes Konto zu erstellen. Geben Sie die Blueprint-Produktinformationen und die Rolleninformationen in die entsprechenden Felder in Account Factory in der AWS Control Tower-Konsole ein, während Sie das Konto erstellen.

Schritt 1. Erstellen Sie die erforderliche Rolle

Bevor Sie mit der Anpassung von Konten beginnen, müssen Sie eine Rolle einrichten, die eine Vertrauensbeziehung zwischen AWS Control Tower und Ihrem Hub-Konto beinhaltet. Wenn die Rolle übernommen wird, gewährt die Rolle dem AWS Control Tower Zugriff zur Verwaltung der Ressourcen im Hub-Konto. Die Rolle muss benannt AWSControlTowerBlueprintAccess werden.

AWS Control Tower übernimmt diese Rolle, um in Ihrem Namen eine Portfolio-Ressource zu erstellen AWS Service Catalog, dann Ihren Blueprint als Service Catalog-Produkt zu diesem Portfolio hinzuzufügen und dann dieses Portfolio und Ihren Blueprint während der Kontobereitstellung mit Ihrem Mitgliedskonto zu teilen.

Sie erstellen die `AWSControlTowerBlueprintAccess` Rolle, wie in den folgenden Abschnitten beschrieben. Sie können die Rolle in einem registrierten oder einem nicht registrierten Konto einrichten.

Navigieren Sie zur IAM-Konsole, um die erforderliche Rolle einzurichten.

Um die AWSControlTowerBlueprintAccess Rolle in einem registrierten AWS Control Tower-Konto einzurichten

1. Verbinden Sie sich mit dem AWS Control Tower-Verwaltungskonto oder melden Sie sich als Principal an.
2. Nehmen Sie vom Verbundprinzipal im Verwaltungskonto aus die `AWSControlTowerExecution` Rolle im registrierten AWS Control Tower-Konto an, das Sie als Blueprint-Hub-Konto ausgewählt haben, oder wechseln Sie zu dieser Rolle.
3. Erstellen Sie aus der `AWSControlTowerExecution` Rolle im registrierten AWS Control Tower-Konto die `AWSControlTowerBlueprintAccess` Rolle mit den richtigen Berechtigungen und Vertrauensbeziehungen.

Important

Um den Richtlinien für AWS bewährte Methoden zu entsprechen, ist es wichtig, dass Sie sich sofort nach dem Erstellen der `AWSControlTowerExecution` Rolle von der `AWSControlTowerBlueprintAccess` Rolle abmelden.
Um unbeabsichtigte Änderungen an Ressourcen zu verhindern, ist die `AWSControlTowerExecution` Rolle nur für die Verwendung durch AWS Control Tower vorgesehen.

Wenn Ihr Blueprint Hub-Konto nicht bei AWS Control Tower registriert ist, ist die `AWSControlTowerExecution` Rolle im Konto nicht vorhanden, und Sie müssen sie nicht übernehmen, bevor Sie mit der Einrichtung der Rolle fortfahren. `AWSControlTowerBlueprintAccess`

Um die AWSControlTowerBlueprintAccess Rolle in einem Mitgliedskonto einzurichten, das nicht registriert ist

1. Verbinden Sie das Konto, das Sie als Hub-Konto festlegen möchten, mit der von Ihnen bevorzugten Methode, oder melden Sie sich als Auftraggeber an.

2. Wenn Sie im Konto als Principal angemeldet sind, erstellen Sie die `AWSControlTowerBlueprintAccess` Rolle mit den entsprechenden Berechtigungen und Vertrauensbeziehungen.

Die AWSControlTowerBlueprintAccess Rolle muss so eingerichtet sein, dass zwei Prinzipalen Vertrauen gewährt wird:

- Der Prinzipal (Benutzer), der AWS Control Tower im AWS Control Tower-Verwaltungskonto ausführt.
- Die `AWSControlTowerAdmin` im AWS Control Tower-Verwaltungskonto angegebene Rolle.

Hier ist ein Beispiel für eine Vertrauensrichtlinie, ähnlich einer, die Sie für Ihre Rolle angeben müssen. Diese Richtlinie zeigt die bewährte Methode zur Gewährung von Zugriffsrechten mit den geringsten Rechten. Wenn Sie Ihre eigene Richtlinie erstellen, ersetzen Sie den Begriff *`YourManagementAccountId`* durch die tatsächliche Konto-ID Ihres AWS Control Tower-Managementkontos und den Begriff *`YourControlTowerUserRole`* durch die ID der IAM-Rolle für Ihr Verwaltungskonto.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": [
                    "arn:aws:iam::111122223333:role/service-role/
AWSControlTowerAdmin",
                    "arn:aws:iam::111122223333:role/YourControlTowerUserRole"
                ]
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

Richtlinie für erforderliche Berechtigungen

Für AWS Control Tower `AWSServiceCatalogAdminFullAccess` muss die angegebene verwaltete Richtlinie der `AWSControlTowerBlueprintAccess` Rolle zugeordnet werden. Diese Richtlinie bietet Berechtigungen, anhand AWS Service Catalog derer geprüft wird, wann AWS Control Tower Ihr Portfolio und Ihre AWS Service Catalog Produktressourcen verwalten darf. Sie können diese Richtlinie anhängen, wenn Sie die Rolle in der IAM-Konsole erstellen.

Möglicherweise sind zusätzliche Berechtigungen erforderlich

- Wenn Sie Ihre Blueprints in Amazon S3 speichern, benötigt AWS Control Tower auch die `AmazonS3ReadOnlyAccess` Berechtigungsrichtlinie für die `AWSControlTowerBlueprintAccess` Rolle.
- Für den AWS Service Catalog Terraform-Produkttyp müssen Sie der benutzerdefinierten AFC-IAM-Richtlinie einige zusätzliche Berechtigungen hinzufügen, wenn Sie nicht die standardmäßige Administratorrichtlinie verwenden. Diese sind zusätzlich zu den Berechtigungen erforderlich, die zum Erstellen der Ressourcen erforderlich sind, die Sie in Ihrer Terraform-Vorlage definieren.

Schritt 2. Erstellen Sie den AWS Service Catalog product

Um ein AWS Service Catalog Produkt zu erstellen, folgen Sie den Schritten unter Produkte erstellen im AWS Service Catalog Administratorhandbuch. Sie fügen Ihren Konto-Blueprint als Vorlage hinzu, wenn Sie das AWS Service Catalog Produkt erstellen.

Important

Aufgrund der HashiCorp aktualisierten Terraform-Lizenzierung wurde die Unterstützung für Terraform Open Source-Produkte und bereitgestellte Produkte auf einen neuen Produkttyp namens Extern AWS Service Catalog umgestellt. Weitere Informationen darüber, wie sich diese Änderung auf AFC auswirkt, einschließlich darüber, wie Sie Ihre bestehenden Konto-Blueprints auf den Produkttyp „Extern“ aktualisieren können, finden Sie unter Umstellung auf den Produkttyp „Extern“. ???

Zusammenfassung der Schritte zur Erstellung eines Blueprints

- Erstellen Sie eine CloudFormation Vorlage oder eine Terraform-Konfigurationsdatei tar.gz, die als Blueprint für Ihr Konto dient, oder laden Sie sie herunter. Einige Vorlagenbeispiele finden Sie weiter unten in diesem Abschnitt.
- Melden Sie sich dort an, AWS-Konto wo Sie Ihre Account Factory-Blueprints speichern (manchmal auch als Hub-Konto bezeichnet).
- Navigieren Sie zur AWS Service Catalog Konsole. Wählen Sie Produktliste und dann Neues Produkt hochladen aus.
- Geben Sie im Bereich Produktdetails Details für Ihr Blueprint-Produkt ein, z. B. einen Namen und eine Beschreibung.
- Wählen Sie Eine Vorlagendatei verwenden und dann Datei auswählen aus. Wählen Sie die Vorlage oder Konfigurationsdatei aus, die Sie zur Verwendung als Blueprint entwickelt oder heruntergeladen haben, oder fügen Sie sie ein.
- Wählen Sie unten auf der Konsolenseite die Option Produkt erstellen aus.

Sie können eine CloudFormation Vorlage aus dem AWS Service Catalog Referenzarchitektur-Repository herunterladen. Ein Beispiel aus diesem Repository hilft bei der Erstellung eines Backup-Plans für Ihre Ressourcen.

Hier ist eine Beispielvorlage für ein fiktives Unternehmen namens Best Pets. Es hilft beim Herstellen einer Verbindung zu ihrer Haustier-Datenbank.

```
Resources:
  ConnectionStringGeneratorLambdaRole:
    Type: AWS::IAM::Role
    Properties:
      AssumeRolePolicyDocument:
        Version: "2012-10-17"
        Statement:
          - Effect: Allow
            Principal:
              Service:
                - lambda.amazonaws.com
            Action:
              - "sts:AssumeRole"
  ConnectionStringGeneratorLambda:
    Type: AWS::Lambda::Function
```

```
    Properties:
      FunctionName: !Join ['-', ['ConnectionStringGenerator', !Select [4, !Split
['-', !Select [2, !Split ['/', !Ref AWS::StackId]]]]]]
      Description: Retrieves the connection string for this account to access the Pet
Database
      Role: !GetAtt ConnectionStringGeneratorLambdaRole.Arn
      Runtime: nodejs22.x
      Handler: index.handler
      Timeout: 5
      Code:
        ZipFile: >
           export const handler = async (event, context) => {
             const awsAccountId = context.invokedFunctionArn.split(":")[4]
             const connectionString= "fake connection for account " + awsAccountId;
             const response = {
               statusCode: 200,
               body: connectionString
             };
            return response;
           };

  ConnectionString:
    Type: Custom::ConnectionStringGenerator
    Properties:
      ServiceToken: !GetAtt ConnectionStringGeneratorLambda.Arn

  PetDatabaseConnectionString:
    DependsOn: ConnectionString
    # For example purposes we're using SSM parameter store.
    # In your template, use secure alternatives to store
    # sensitive values such as connection strings.
    Type: AWS::SSM::Parameter
    Properties:
      Name: pet-database-connection-string
      Description: Connection information for the BestPets pet database
      Type: String
      Value: !GetAtt ConnectionString.Value
```

Schritt 3. Überprüfe deinen benutzerdefinierten Blueprint

Sie können Ihren Blueprint in der AWS Service Catalog Konsole anzeigen. Weitere Informationen finden Sie unter Produkte verwalten im Service Catalog Adminstrator Guide.

Schritt 4. Rufen Sie Ihren Blueprint auf, um ein benutzerdefiniertes Konto zu erstellen

Wenn Sie dem Workflow „Konto erstellen“ in der AWS Control Tower-Konsole folgen, wird ein optionaler Abschnitt angezeigt, in dem Sie Informationen zu dem Blueprint eingeben können, den Sie für die Anpassung von Konten verwenden möchten.

> **Voraussetzungen**
>
> Sie müssen Ihr Customization Hub-Konto einrichten und mindestens einen Blueprint (Service Catalog-Produkt) hinzufügen, bevor Sie diese Informationen in die AWS Control Tower-Konsole eingeben und mit der Bereitstellung benutzerdefinierter Konten beginnen können.

Erstellen oder aktualisieren Sie ein benutzerdefiniertes Konto in der AWS Control Tower-Konsole.

1. Geben Sie die Konto-ID für das Konto ein, das Ihre Blueprints enthält.
2. Wählen Sie in diesem Konto ein vorhandenes Service Catalog-Produkt (vorhandener Blueprint) aus.
3. Wählen Sie die richtige Version des Blueprints (Service Catalog-Produkt) aus, wenn Sie mehr als eine Version haben.
4. (Optional) Sie können zu diesem Zeitpunkt des Prozesses eine Blueprint-Bereitstellungsrichtlinie hinzufügen oder ändern. Die Blueprint-Bereitstellungsrichtlinie ist in JSON geschrieben und an eine IAM-Rolle angehängt, sodass sie die in der Blueprint-Vorlage angegebenen Ressourcen bereitstellen kann. AWS Control Tower erstellt diese Rolle im Mitgliedskonto, sodass Service Catalog Ressourcen mithilfe von Stack-Sets bereitstellen kann. CloudFormation Der Name der Rolle lautet `AWSControlTower-BlueprintExecution-bp-`*`xxxx`*. Die `AdministratorAccess` Richtlinie wird hier standardmäßig angewendet.
5. Wählen Sie die AWS-Region oder Regionen aus, in denen Sie Konten auf der Grundlage dieses Blueprints bereitstellen möchten.
6. Wenn Ihr Blueprint Parameter enthält, können Sie die Werte für die Parameter in zusätzliche Felder im AWS Control Tower-Workflow eingeben. Zu den zusätzlichen Werten können gehören: ein GitHub Repository-Name, ein GitHub Branch, ein Amazon ECS-Clustername und eine GitHub Identität für den Repository-Besitzer.
7. Sie können Konten zu einem späteren Zeitpunkt anpassen, indem Sie dem Kontoaktualisierungsprozess folgen, falls Ihr Hub-Konto oder Ihre Blueprints noch nicht bereit sind.

Weitere Details finden Sie unter Erstellen Sie ein benutzerdefiniertes Konto anhand eines Blueprints.

Erstellen Sie ein benutzerdefiniertes Konto anhand eines Blueprints

Nachdem Sie benutzerdefinierte Blueprints erstellt haben, können Sie mit der Erstellung benutzerdefinierter Konten in der AWS Control Tower Account Factory beginnen.

Folgen Sie diesen Schritten, um einen benutzerdefinierten Blueprint bereitzustellen, wenn Sie einen neuen erstellen AWS Konto:

1. Gehen Sie zum AWS Control Tower im AWS-Managementkonsole.
2. Wählen Sie Account Factory und dann Konto erstellen aus.
3. Geben Sie Kontodetails wie Kontoname und E-Mail-Adresse ein.
4. Konfigurieren Sie die IAM Identity Center-Details mit E-Mail-Adresse und Benutzername.
5. Wählen Sie eine registrierte OU aus, zu der Ihr Konto hinzugefügt werden soll.
6. Erweitere den Abschnitt Factory-Anpassung des Accounts.
7. Geben Sie die Konto-ID des Blueprint Hub-Kontos ein, das Ihre Service Catalog-Produkte enthält, und wählen Sie Validieren aus. Weitere Informationen zu einem Blueprint Hub-Konto finden Sie unter. Passen Sie Konten mit Account Factory Customization (AFC) an
8. Wählen Sie das Dropdownmenü aus, das alle Blueprints aus Ihrer Service Catalog-Produktliste enthält (alle benutzerdefinierten Blueprints und Partner-Blueprints). Wählen Sie einen Blueprint und die entsprechende Version für die Bereitstellung aus.
9. Wenn Ihr Blueprint Parameter enthält, werden diese Felder angezeigt, damit Sie sie ausfüllen können. Die Standardwerte sind vorab ausgefüllt.
10. Wählen Sie abschließend aus, wo Sie Ihren Blueprint bereitstellen möchten, entweder Heimatregion oder Alle kontrollierten Regionen. Globale Ressourcen wie Route 53 oder IAM müssen möglicherweise nur in einer einzigen Region bereitgestellt werden. Regionale Ressourcen wie Amazon EC2-Instances oder Amazon S3-Buckets könnten in allen regierten Regionen bereitgestellt werden
11. Nachdem alle Felder ausgefüllt sind, wählen Sie Konto erstellen aus.

> **Note**
>
> Mit Terraform erstellte Blueprints können nur in einer Region bereitgestellt werden, nicht in mehreren Regionen.

Sie können den Fortschritt Ihrer Kontobereitstellung auf der Seite Organisation einsehen. Wenn Ihre Kontobereitstellung abgeschlossen ist, sind die in Ihrem Blueprint angegebenen Ressourcen bereits darin bereitgestellt. Um die Details des Kontos und des Blueprints anzuzeigen, gehen Sie zur Seite mit den Kontodetails.

Passen Sie Konten bei AFC an, während Sie sie registrieren

Um Konten in der AWS Control Tower-Konsole zu registrieren und anzupassen.

1. Navigieren Sie zur AWS Control Tower-Konsole und wählen Sie im linken Navigationsbereich Organisation aus.
2. Sie sehen eine Liste Ihrer verfügbaren Konten. Identifizieren Sie das Konto, das Sie registrieren möchten, mit einem benutzerdefinierten Blueprint. In der Spalte Bundesland für dieses Konto sollte das Konto mit dem Status Nicht registriert angezeigt werden.
3. Wählen Sie das Optionsfeld links neben dem Konto aus und wählen Sie das Dropdownmenü Aktionen oben rechts auf dem Bildschirm. Hier wählen Sie die Option Registrieren.
4. Füllen Sie den Abschnitt Zugriffskonfiguration mit den IAM Identity Center-Informationen des Kontos aus.
5. Wählen Sie die registrierte OU aus, in der Ihr Konto Mitglied werden soll.
6. Füllen Sie den Abschnitt Factory-Anpassung des Accounts aus, indem Sie dieselben Schritte wie in den Schritten 7-12 des Verfahrens Konto erstellen ausführen. Weitere Informationen findest du unter Bereitstellen von Account Factory-Konten mit AWS Service Catalog.

Den Status Ihres Kontofortschritts können Sie auf der Seite Organisation einsehen. Wenn Ihre Kontoregistrierung abgeschlossen ist, sind die im Blueprint angegebenen Ressourcen bereits darin bereitgestellt.

Fügen Sie einem AWS Control Tower-Konto einen Blueprint hinzu

Um einem bestehenden AWS Control Tower-Mitgliedskonto einen Blueprint hinzuzufügen, folgen Sie dem Workflow Konto aktualisieren in der AWS Control Tower-Konsole und wählen Sie einen neuen Blueprint aus, der dem Konto hinzugefügt werden soll. Weitere Informationen finden Sie unter Account Factory-Konten mit AWS Control Tower oder mit aktualisieren und verschieben. AWS Service Catalog

> **Note**
>
> Wenn Sie einem Konto einen neuen Blueprint hinzufügen, wird der vorhandene Blueprint überschrieben.

> **Note**
>
> Ein Blueprint kann pro AWS Control Tower-Konto bereitgestellt werden.

Aktualisieren Sie einen Blueprint

In den folgenden Verfahren wird beschrieben, wie benutzerdefinierte Blueprints aktualisiert und bereitgestellt werden.

Um Ihre benutzerdefinierten Blueprints zu aktualisieren

1. Aktualisieren Sie Ihre CloudFormation Vorlage oder Terraform-Datei tar.gz (Blueprint) mit Ihren neuen Konfigurationen.
2. Speichern Sie den aktualisierten Blueprint als neue Version in. AWS Service Catalog

Um Ihren aktualisierten Blueprint bereitzustellen

1. Navigieren Sie in der AWS Control Tower-Konsole zur Seite Organisation.
2. Filtern Sie die Organisationsseite nach Blueprint-Name und Version.
3. Folgen Sie dem Vorgang Konto aktualisieren und stellen Sie die neueste Blueprint-Version in Ihrem Konto bereit.

Wenn ein Blueprint-Update nicht erfolgreich ist

AWS Control Tower ermöglicht Blueprint-Updates, wenn sich das bereitgestellte Produkt im Status befindet. `AVAILABLE` Wenn sich Ihr bereitgestelltes Produkt in einem `TAINTED` Status befindet, schlägt das Update fehl. Wir empfehlen die folgende Problemumgehung:

1. Aktualisieren Sie das `TAINTED` bereitgestellte Produkt in der AWS Service Catalog Konsole manuell, um den Status auf zu ändern. `AVAILABLE` Weitere Informationen finden Sie unter Aktualisieren bereitgestellter Produkte.
2. Folgen Sie dann dem Vorgang zur Kontoaktualisierung im AWS Control Tower, um den Blueprint-Bereitstellungsfehler zu beheben.

Wir empfehlen diesen manuellen Schritt aus folgenden Gründen: Wenn Sie einen Blueprint entfernen, kann dies dazu führen, dass Ressourcen im Mitgliedskonto entfernt werden. Das Entfernen von Ressourcen kann sich auf Ihre vorhandenen Workloads auswirken. Aus diesem Grund empfehlen wir diese Methode und nicht die alternative Methode der Aktualisierung eines Blueprints, bei der der ursprüngliche Blueprint entfernt und ersetzt wird, insbesondere, wenn Sie Produktions-Workloads ausführen.

Einen Blueprint aus einem Konto entfernen

Um einen Blueprint aus einem Konto zu entfernen, folgen Sie dem Workflow „Konto aktualisieren“, um den Blueprint zu entfernen und das Konto auf die AWS Control Tower-Standardkonfigurationen zurückzusetzen.

Wenn Sie den Workflow zur Kontoaktualisierung in der Konsole aufrufen, werden Sie feststellen, dass alle Kontodetails ausgefüllt sind und die Anpassungsdetails nicht ausgefüllt sind. Wenn Sie diese AFC-Details leer lassen, entfernt AWS Control Tower den Blueprint aus dem Konto. Bevor die Aktion beginnt, wird eine Warnmeldung angezeigt.

> **Note**
>
> AWS Control Tower fügt einem Konto nur dann einen Blueprint hinzu, wenn Sie während des Prozesses Konto erstellen oder Konto aktualisieren einen Blueprint auswählen.

Pläne von Partnern

AWS Control Tower Account Factory Customization (AFC) bietet Zugriff auf vordefinierte Anpassungs-Blueprints, die von Partnern erstellt und verwaltet werden. AWS Diese Partner-Blueprints helfen Ihnen dabei, Ihre Konten an bestimmte Anwendungsfälle anzupassen. Die Blueprints der einzelnen Partner helfen Ihnen dabei, maßgeschneiderte Konten zu erstellen, die so vorkonfiguriert sind, dass sie mit den Produktangeboten des jeweiligen Partners kompatibel sind.

Eine vollständige Liste der AWS Control Tower-Partner-Blueprints finden Sie in Ihrer Konsole in der Service Catalog-Bibliothek „Erste Schritte“. Suchen Sie nach dem Quelltyp AWS Control Tower Blueprints.

Überlegungen zu Account Factory-Anpassungen (AFC)

- AFC unterstützt Anpassungen nur mit einem einzigen AWS Service Catalog Blueprint-Produkt.
- Die AWS Service Catalog Blueprint-Produkte müssen im Hub-Konto und in derselben Region wie die Heimatregion der AWS Control Tower-Landing Zone erstellt werden.
- Die `AWSControlTowerBlueprintAccess` IAM-Rolle muss mit dem richtigen Namen, den richtigen Berechtigungen und der Vertrauensrichtlinie erstellt werden.
- AWS Control Tower unterstützt zwei Bereitstellungsoptionen für Blueprints: Bereitstellung nur in der Heimatregion oder Bereitstellung in allen Regionen, die vom AWS Control Tower verwaltet werden. Die Auswahl der Regionen ist nicht verfügbar.
- Wenn Sie einen Blueprint in einem Mitgliedskonto aktualisieren, können die Blueprint-Hub-Konto-ID und das AWS Service Catalog Blueprint-Produkt nicht geändert werden.
- AWS Control Tower unterstützt nicht das Entfernen eines vorhandenen Blueprints und das Hinzufügen eines neuen Blueprints in einem einzigen Blueprint-Aktualisierungsvorgang. Sie können einen Blueprint entfernen und dann in separaten Vorgängen einen neuen Blueprint hinzufügen.
- AWS Control Tower ändert das Verhalten, je nachdem, ob Sie benutzerdefinierte Konten oder nicht benutzerdefinierte Konten erstellen oder registrieren. Wenn Sie keine benutzerdefinierten Konten mit Blueprints erstellen oder registrieren, erstellt AWS Control Tower ein von Account Factory bereitgestelltes Produkt (über Service Catalog) im AWS Control Tower-Managementkonto. Wenn Sie bei der Erstellung oder Registrierung von Konten mit Blueprints Anpassungen angeben, erstellt AWS Control Tower kein von Account Factory bereitgestelltes Produkt im AWS Control Tower-Verwaltungskonto.

Im Falle eines Blueprint-Fehlers

Fehler beim Anwenden eines Blueprints

Wenn beim Anwenden eines Blueprints auf ein Konto — entweder ein neues Konto oder ein vorhandenes Konto, das Sie bei AWS Control Tower registrieren — ein Fehler auftritt, ist das Wiederherstellungsverfahren dasselbe. Das Konto wird existieren, aber es ist nicht angepasst und es ist nicht bei AWS Control Tower registriert. Um fortzufahren, folgen Sie den Schritten zur

Registrierung des Kontos bei AWS Control Tower und fügen Sie den Blueprint bei der Registrierung hinzu.

Fehler beim Erstellen der Rolle und Problemumgehungen **`AWSControlTowerBlueprintAccess`**

Wenn Sie die `AWSControlTowerBlueprintAccess` Rolle von einem AWS Control Tower-Konto aus erstellen, müssen Sie als Principal angemeldet sein, der die Rolle verwendet. `AWSControlTowerExecution` Wenn Sie als ein anderer Benutzer angemeldet sind, wird der `CreateRole` Vorgang durch einen SCP verhindert, wie das folgende Artefakt zeigt:

```
{
            "Condition": {
                "ArnNotLike": {
                    "aws:PrincipalArn": [
                        "arn:aws:iam::*:role/AWSControlTowerExecution",
                        "arn:aws:iam::*:role/stacksets-exec-*"
                    ]
                }
            },
            "Action": [
                "iam:AttachRolePolicy",
                "iam:CreateRole",
                "iam:DeleteRole",
                "iam:DeleteRolePermissionsBoundary",
                "iam:DeleteRolePolicy",
                "iam:DetachRolePolicy",
                "iam:PutRolePermissionsBoundary",
                "iam:PutRolePolicy",
                "iam:UpdateAssumeRolePolicy",
                "iam:UpdateRole",
                "iam:UpdateRoleDescription"
            ],
            "Resource": [
                "arn:aws:iam::*:role/aws-controltower-*",
                "arn:aws:iam::*:role/*AWSControlTower*",
                "arn:aws:iam::*:role/stacksets-exec-*"
            ],
            "Effect": "Deny",
            "Sid": "GRIAMROLEPOLICY"
        }
```

Die folgenden Problemumgehungen sind verfügbar:

- (Am meisten empfohlen) Übernehmen Sie die `AWSControlTowerExecution` Rolle und erstellen Sie die `AWSControlTowerBlueprintAccess` Rolle. Wenn Sie sich für diese Problemumgehung entscheiden, stellen Sie sicher, dass Sie sich unmittelbar danach von der `AWSControlTowerExecution` Rolle abmelden, um unbeabsichtigte Änderungen an den Ressourcen zu verhindern.
- Melden Sie sich mit einem Konto an, das nicht bei AWS Control Tower registriert ist und daher nicht diesem SCP unterliegt.
- Bearbeiten Sie diesen SCP vorübergehend, um den Vorgang zuzulassen.
- (Dringend nicht empfohlen) Verwenden Sie Ihr AWS Control Tower-Managementkonto als Ihr Hub-Konto, damit es nicht dem SCP unterliegt.

Anpassung Ihres Richtliniendokuments für AFC-Blueprints auf der Grundlage von CloudFormation

Wenn Sie einen Blueprint über Account Factory aktivieren, weist AWS Control Tower an, einen StackSet Blueprint in Ihrem CloudFormation Namen zu erstellen. CloudFormation benötigt Zugriff auf Ihr verwaltetes Konto, um CloudFormation Stacks in der zu erstellen. StackSet Zwar verfügt die `AWSControlTowerExecution` Rolle CloudFormation bereits über Administratorrechte im verwalteten Konto, diese Rolle kann jedoch nicht übernommen werden. CloudFormation

Im Rahmen der Aktivierung eines Blueprints erstellt AWS Control Tower eine Rolle im Mitgliedskonto, das CloudFormation möglicherweise die Ausführung der StackSet Verwaltungsaufgaben übernimmt. Die einfachste Methode, Ihren benutzerdefinierten Blueprint über Account Factory zu aktivieren, ist die Verwendung einer Allowall-Richtlinie, da diese Richtlinien mit jeder Blueprint-Vorlage kompatibel sind.

Bewährte Methoden empfehlen jedoch, dass Sie die Berechtigungen für CloudFormation das Zielkonto einschränken müssen. Sie können eine benutzerdefinierte Richtlinie angeben, die AWS Control Tower auf die Rolle anwendet, für die es erstellt wurde, um sie CloudFormation zu verwenden. Wenn Ihr Blueprint beispielsweise einen SSM-Parameter mit dem Namen something-important erstellt, könnten Sie die folgende Richtlinie angeben:

JSON

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

```
    "Statement": [
        {
            "Sid": "AllowCloudFormationActionsOnStacks",
            "Effect": "Allow",
            "Action": "cloudformation:*",
            "Resource": "arn:aws:cloudformation:*:*:stack/*"
        },
        {
            "Sid": "AllowSsmParameterActions",
            "Effect": "Allow",
            "Action": [
                "ssm:PutParameter",
                 "ssm:DeleteParameter",
                 "ssm:GetParameter",
                 "ssm:GetParameters"
            ],
            "Resource": "arn:*:ssm:*:*:parameter/something-important"
        }
    ]
}
```

Die `AllowCloudFormationActionsOnStacks` Anweisung ist für alle benutzerdefinierten AFC-Richtlinien erforderlich. Sie CloudFormation verwendet diese Rolle, um Stack-Instances zu erstellen. Daher ist die Berechtigung zum Ausführen von Aktionen auf Stacks erforderlich. CloudFormation Der `AllowSsmParameterActions` Abschnitt bezieht sich speziell auf die Vorlage, die aktiviert wird.

Lösen Sie Probleme mit der Zugriffsberechtigung

Wenn Sie einen Blueprint mit einer eingeschränkten Richtlinie aktivieren, stellen Sie möglicherweise fest, dass nicht genügend Berechtigungen vorhanden sind, um den Blueprint zu aktivieren. Um diese Probleme zu beheben, überarbeiten Sie Ihr Richtliniendokument und aktualisieren Sie die Blueprint-Einstellungen des Mitgliedskontos, sodass die korrigierte Richtlinie verwendet wird. Um zu überprüfen, ob die Richtlinie ausreicht, um den Blueprint zu aktivieren, stellen Sie sicher, dass die CloudFormation Berechtigungen erteilt wurden und dass Sie direkt mithilfe dieser Rolle einen Stack erstellen können.

Für die Erstellung eines Terraform-based Service Catalog-Produkts sind zusätzliche Berechtigungen erforderlich

Wenn Sie ein AWS Service Catalog externes Produkt mit einer Terraform-Konfigurationsdatei für AFC erstellen, AWS Service Catalog müssen Ihrer benutzerdefinierten AFC-IAM-Richtlinie zusätzlich zu den Berechtigungen, die zum Erstellen der in Ihrer Vorlage definierten Ressourcen erforderlich sind, bestimmte Berechtigungen hinzugefügt werden. Wenn Sie die standardmäßige vollständige Administratorrichtlinie wählen, müssen Sie diese zusätzlichen Berechtigungen nicht hinzufügen.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Action": [
                "resource-groups:CreateGroup",
                "resource-groups:ListGroupResources",
                "resource-groups:DeleteGroup",
                "resource-groups:Tag"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "tag:GetResources",
                "tag:GetTagKeys",
                "tag:GetTagValues",
                "tag:TagResources",
                "tag:UntagResources"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": "s3:GetObject",
            "Effect": "Allow",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
```

```
                    "s3:ExistingObjectTag/servicecatalog:provisioning": "true"
                }
            }
        }
    ]
}
```

Weitere Informationen zum Erstellen von Terraform-Produkten mit dem Produkttyp „External“ finden Sie unter Schritt 5: Startrollen erstellen im Service Catalog-Administratorhandbuch. AWS Service Catalog

Übergang zum AWS Service Catalog Externer Produkttyp

AWS Service Catalog Die Unterstützung für Terraform Open Source-Produkte und bereitgestellte Produkte wurde auf einen neuen Produkttyp namens External geändert. Weitere Informationen zu dieser Umstellung finden Sie im Administratorhandbuch unter Aktualisierung vorhandener Terraform Open Source-Produkte und bereitgestellter Produkte auf den Produkttyp Extern. AWS Service Catalog

Diese Änderung wirkt sich auf bestehende Konten aus, die Sie mit der werkseitigen Anpassung des AWS Control Tower-Kontos erstellt oder registriert haben. Um diese Konten auf den Produkttyp Extern umzustellen, müssen Sie sowohl in AWS Control Tower als auch AWS Service Catalog in AWS Control Tower Änderungen vornehmen.

Um zum Produkttyp Extern überzugehen

1. Aktualisieren Sie Ihre bestehende Terraform Reference Engine so, dass sie sowohl AWS Service Catalog den externen als auch den Terraform Open Source-Produkttypen unterstützt. Anweisungen zur Aktualisierung Ihrer Terraform Reference Engine finden Sie im Repository. AWS Service Catalog GitHub
2. AWS Service Catalog Duplizieren Sie in alle vorhandenen Terraform Open Source-Produkte (Blueprints), wobei die Duplikate den neuen externen Produkttyp verwenden. Beenden Sie nicht die vorhandenen Terraform Open Source-Blueprints.
3. Aktualisieren Sie im AWS Control Tower jedes Konto mithilfe eines Terraform Open Source-Blueprints, um den neuen externen Blueprint zu verwenden.

a. Um einen Blueprint zu aktualisieren, müssen Sie zuerst den Terraform Open Source-Blueprint vollständig entfernen. Weitere Informationen finden Sie unter Einen Blueprint aus einem Konto entfernen.

b. Fügen Sie den neuen externen Blueprint demselben Konto hinzu. Weitere Informationen finden Sie unter Einen Blueprint zu einem AWS Control Tower-Konto hinzufügen.

4. Nachdem alle Konten, die Terraform Open Source-Blueprints verwenden, auf Externe Blueprints aktualisiert wurden, kehren Sie zu allen Produkten zurück, die Terraform Open Source als Produkttyp verwenden, AWS Service Catalog und kündigen Sie diese.

5. In Zukunft müssen alle Konten, die mithilfe der werkseitigen Anpassung des AWS-Control-Tower-Kontos erstellt oder registriert wurden, auf Blueprints verweisen, die den Produkttyp oder External verwenden. CloudFormation

   Für Blueprints, die mit dem Produkttyp External erstellt wurden, unterstützt AWS Control Tower nur Kontoanpassungen, die Terraform-Vorlagen und die Terraform-Referenz-Engine verwenden. Weitere Informationen finden Sie unter Zur Anpassung einrichten. https://docs.aws.amazon.com/controltower/latest/userguide/afc-setup-steps.html

> **Note**
>
> AWS Control Tower unterstützt Terraform Open Source als Produkttyp bei der Erstellung neuer Konten nicht. Weitere Informationen zu diesen Änderungen finden Sie im Administratorhandbuch unter Aktualisierung vorhandener Terraform Open Source-Produkte und bereitgestellter Produkte auf den Produkttyp Extern. AWS Service Catalog AWS Service Catalog unterstützt Kunden bei Bedarf bei der Umstellung des Produkttyps. Wenden Sie sich an Ihren Kundenbetreuer, um Unterstützung anzufordern.

Bereitstellung von Konten mit AWS Control Tower Account Factory für Terraform (AFT)

AWS Control Tower Account Factory for Terraform (AFT) verwendet ein GitOps Modell, das den Prozess der Kontobereitstellung und -aktualisierung in AWS Control Tower automatisiert.

Mit AFT erstellen Sie eine Terraform-Datei zur Kontoanforderung, die die Eingabe enthält, die den AFT-Workflow aufruft. Nach Abschluss der Kontobereitstellung und -aktualisierung wird der

AFT-Workflow fortgesetzt, indem das AFT-Kontobereitstellungsframework und die Schritte zur Kontoanpassung ausgeführt werden.

AFT hat keinen Einfluss auf die Workflow-Leistung im AWS Control Tower. Wenn Sie ein Konto über AFT oder Account Factory bereitstellen, findet derselbe Backend-Workflow statt.

Voraussetzungen

> **Note**
>
> Die Bereitstellung eines AFT-Kontos muss auf eine Organisationseinheit (OU) abzielen, die im AWS Control Tower AWSControlTowerBaseline aktiviert ist. Einzelheiten finden Sie AWSControlTowerBaseline unter:Basistypen, die auf OU-Ebene gelten.

Wenn Sie mit AFT beginnen, erstellen Sie Folgendes:

- Erstellen Sie im AWS Control Tower die Organisationseinheit und dann das AFT-Verwaltungskonto für Ihre AFT-Umgebung. Notieren Sie sich die Konto-ID, damit Sie sie später in die `main.tf` Datei eingeben können, wenn Sie AFT mit dem Terraform-Modul bereitstellen. Sie können diese Konto-ID auf der Detailseite von AWS Control Tower Control einsehen. Weitere Informationen finden Sie in der Terraform-Dokumentation.
- Ein oder mehrere `git` Repositorys für Ihre vollständig bereitgestellte AFT-Umgebung. Weitere Informationen finden Sie unter Post-deployment Schritte für AFT.
- Eine vollständig bereitgestellte AFT-Umgebung. Weitere Informationen finden Sie unter Überblick über AWS Control Tower Account Factory for Terraform (AFT) und Deploy AWS Control Tower Account Factory for Terraform (AFT). Siehe auch die Terraform-Dokumentation.

> **Tip**
>
> Sie können das AFT-Verwaltungskonto von der AWS Control Tower-Konsole aus mit Konto erstellen erstellen. Weitere Informationen finden Sie unter https://docs.aws.amazon.com/controltower/latest/userguide/methods-of-provisioning.html Bereitstellungsmethoden. Optional können Sie im Repository aft-account-customizations auch einen Ordner mit Kontovorlagen erstellen, der Ihnen bei der Definition Ihrer zusätzlichen Konten hilft.

Für Konten, die über die automatische Registrierung registriert wurden:

- Die Erstellung neuer Konten über AFT funktioniert weiterhin normal.
- Für den Import vorhandener Konten sind zusätzliche Schritte erforderlich:
  - Registrieren Sie OU, um vor dem Import die erforderlichen bereitgestellten Produkte zu erstellen.
  - Die Register-OU sendet `UpdateManagedAccount` Ereignisse aus `CreateManagedAccount` und ermöglicht so AFT-Anpassungen.

Informationen dazu AWS-Regionen , wo AFT Einsatzbeschränkungen hat, finden Sie unter Einschränkungen und Kontingente in AWS Control Tower undEinschränkungen bei der Steuerung.

Die Terraform-Dokumentation enthält einen guten Überblick über die Einrichtung von AWS Control Tower Account Factory for Terraform (AFT).

Überblick über AWS Control Tower Account Factory für Terraform (AFT)

Account Factory for Terraform (AFT) richtet eine Terraform-Pipeline ein, die Sie bei der Bereitstellung und Anpassung von Konten im AWS Control Tower unterstützt. AFT bietet Ihnen den Vorteil der Terraform-based Kontobereitstellung und ermöglicht Ihnen gleichzeitig, Ihre Konten mit AWS Control Tower zu verwalten.

Mit AFT erstellen Sie eine Terraform-Datei zur Kontoanforderung, um die Eingabe zu erhalten, die den AFT-Workflow für die Kontobereitstellung auslöst. Nach Abschluss der Kontobereitstellungsphase führt AFT automatisch eine Reihe von Schritten aus, bevor die Phase der Kontoanpassungen beginnt. Weitere Informationen finden Sie unter AFT-Kontobereitstellungspipeline.

AFT unterstützt HCP Terraform, Terraform Enterprise und Terraform Community Edition. Mit AFT können Sie mithilfe einer Eingabedatei und einem einfachen `git push` Befehl die Kontoerstellung initiieren und neue oder bestehende Konten anpassen. Die Kontoerstellung beinhaltet alle Verwaltungsvorteile von AWS Control Tower sowie die Kontoanpassungen, mit denen Sie die Standardsicherheitsverfahren und Compliance-Richtlinien Ihres Unternehmens einhalten können.

AFT unterstützt die Nachverfolgung von Anfragen zur Kontoanpassung. Jedes Mal, wenn Sie eine Anfrage zur Kontoanpassung einreichen, generiert AFT ein eindeutiges Ablaufverfolgungstoken, das eine AWS Step Functions AFT-Zustandsmaschine durchläuft, die das Token im Rahmen seiner Ausführung protokolliert. Anschließend können Sie Amazon CloudWatch Logs Insights-Abfragen verwenden, um Zeitstempelbereiche zu durchsuchen und das Anforderungstoken abzurufen.

Dadurch können Sie die Payloads sehen, die dem Token beiliegen, sodass Sie Ihre Anfrage zur Kontoanpassung während des gesamten AFT-Workflows verfolgen können. Informationen zu CloudWatch Logs und Step Functions finden Sie im Folgenden:

- Was ist Amazon CloudWatch Logs? im Amazon CloudWatch Logs-Benutzerhandbuch
- Was ist AWS Step Functions? im Entwicklerhandbuch für AWS Step Functions

AFT kombiniert die Funktionen anderer AWS DiensteKomponentendienste, z. B. um ein Framework zu erstellen, mit Pipelines, die Terraform Infrastructure as Code (IaC) bereitstellen. AFT ermöglicht Ihnen:

- Anfragen zur Kontobereitstellung und Aktualisierung in einem GitOps Modell einreichen
- Speichern Sie Konto-Metadaten und den Auditverlauf
- Wenden Sie Tags auf Kontoebene an
- Fügen Sie Anpassungen zu allen Konten, zu einer Gruppe von Konten oder zu einzelnen Konten hinzu
- Aktivieren Sie die Funktionsoptionen

AFT erstellt ein separates Konto, das sogenannte AFT-Verwaltungskonto, um AFT-Funktionen bereitzustellen. Bevor Sie AFT einrichten können, müssen Sie über eine bestehende AWS Control Tower-Landezone verfügen. Das AFT-Verwaltungskonto ist nicht dasselbe wie das AWS Control Tower-Verwaltungskonto.

AFT bietet Flexibilität

- Flexibilität für Ihre Plattform: AFT unterstützt jede Terraform-Distribution für die Erstbereitstellung und den laufenden Betrieb: Community Edition, Cloud und Enterprise.
- Flexibilität für Ihr Versionskontrollsystem: AFT unterstützt AWS CodeCommit und bietet alternative Versionskontrollquellen. AWS CodeConnections

AFT bietet Funktionsoptionen

Sie können verschiedene Funktionsoptionen aktivieren, die auf bewährten Methoden basieren:

- Erstellung einer Organisationsebene CloudTrail für die Protokollierung von Datenereignissen
- Löschen der AWS Standard-VPC für Konten

- Registrierung bereitgestellter Konten für den Enterprise Support-Plan AWS

> **Note**
>
> Die AFT-Pipeline ist nicht für die Bereitstellung von Ressourcen wie Amazon EC2-Instances vorgesehen, die Ihre Konten für die Ausführung Ihrer Anwendungen benötigen. Sie ist ausschließlich für die automatische Bereitstellung und Anpassung von AWS Control Tower-Konten vorgesehen.

Video-Anleitung

Dieses Video (7:33) beschreibt, wie Konten mit AWS Control Tower Account Factory für Terraform bereitgestellt werden. Wählen Sie zur besseren Ansicht das Symbol in der rechten unteren Ecke des Videos, um es in voller Bildschirmgröße anzuzeigen. Es stehen Untertitel zur Verfügung.

Video-Walkthrough zur automatisierten Kontobereitstellung in AWS Control Tower.

AFT-Architektur

Reihenfolge der Operationen

Sie führen AFT-Operationen im AFT-Verwaltungskonto aus. Für einen vollständigen Workflow zur Kontobereitstellung sind die Stufen im Diagramm von links nach rechts wie folgt angeordnet:

1. Kontoanfragen werden erstellt und an die Pipeline übermittelt. Sie können mehrere Kontoanfragen gleichzeitig erstellen und einreichen. Account Factory verarbeitet Anfragen in einer First-in-First-Out-Reihenfolge. Weitere Informationen finden Sie unter Mehrere Kontoanfragen einreichen.
2. Jedes Konto wird bereitgestellt. Diese Phase wird im AWS Control Tower-Verwaltungskonto ausgeführt.
3. Globale Anpassungen werden in den Pipelines ausgeführt, die für jedes verkaufte Konto erstellt werden.
4. Wenn Anpassungen in den ursprünglichen Kontobereitstellungsanforderungen angegeben sind, werden die Anpassungen nur für Zielkonten ausgeführt. Wenn Sie ein Konto haben, das bereits bereitgestellt wurde, müssen Sie weitere Anpassungen manuell in der Pipeline des Kontos vornehmen.

AWS Control Tower Account Factory für Terraform — Workflow zur Kontobereitstellung

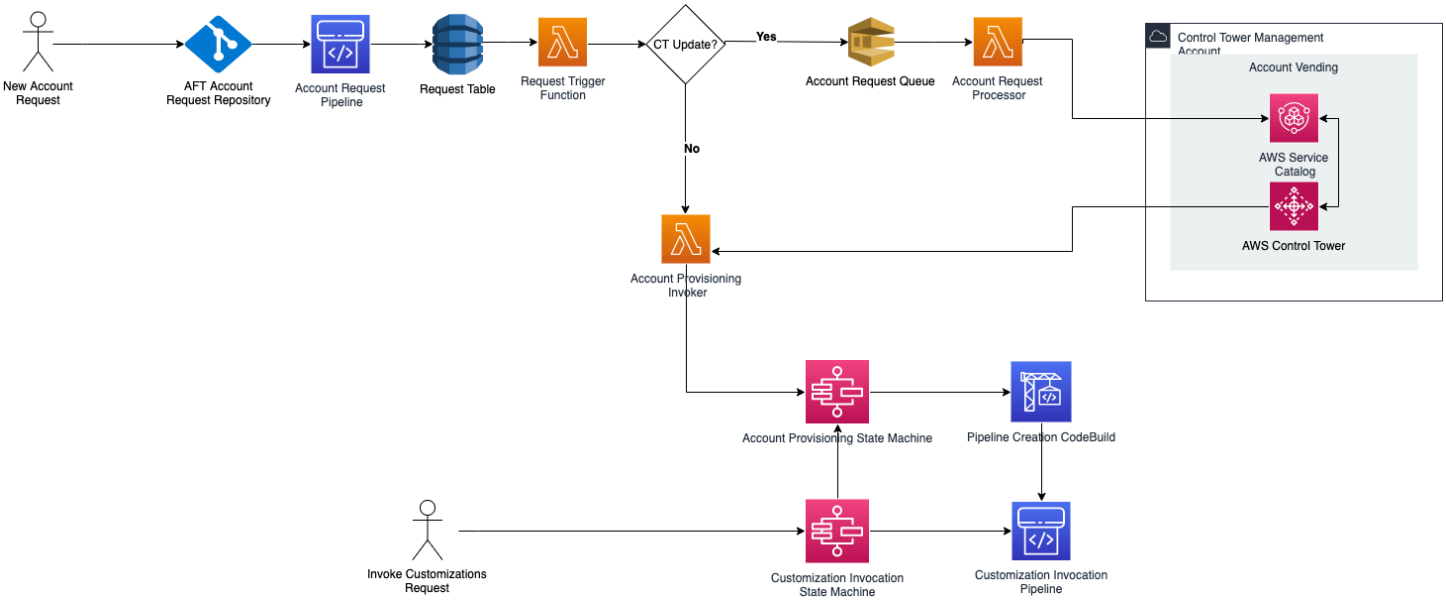

Abbildung 1: AWS Control Tower Account Factory für Terraform

Cost (Kosten)

Für AFT fallen keine zusätzlichen Gebühren an. Sie zahlen nur für die von AFT bereitgestellten Ressourcen, die von AFT aktivierten AWS Dienste und die Ressourcen, die Sie in Ihrer AFT-Umgebung bereitstellen.

Die standardmäßige AFT-Konfiguration umfasst die Zuweisung von AWS PrivateLink Endpunkten für verbesserten Datenschutz und Sicherheit sowie ein NAT-Gateway, das zur Unterstützung AWS CodeBuild erforderlich ist. Einzelheiten zur Preisgestaltung dieser Infrastruktur finden Sie in der AWS PrivateLink Preisgestaltung und in den Amazon VPC-Preisen für das NAT Gateway. Weitere Informationen zur Verwaltung dieser Kosten erhalten Sie von Ihrem AWS Kundenbetreuer. Sie können diese Standardeinstellungen für AFT ändern.

Stellen Sie AWS Control Tower Account Factory für Terraform (AFT) bereit

Dieser Abschnitt richtet sich an Administratoren von AWS Control Tower Tower-Umgebungen, die Account Factory for Terraform (AFT) in ihrer bestehenden Umgebung einrichten möchten. Es beschreibt, wie Sie eine Account Factory for Terraform (AFT) -Umgebung mit einem neuen, dedizierten AFT-Verwaltungskonto einrichten.

> **Note**
>
> Ein Terraform-Modul stellt AFT bereit. Dieses Modul ist im AFT-Repository am verfügbar GitHub, und das gesamte AFT-Repository wird als Modul betrachtet.
> Wir empfehlen, dass Sie auf die AFT-Module verweisen, GitHub anstatt das AFT-Repository zu klonen. Auf diese Weise können Sie Updates für die Module kontrollieren und nutzen, sobald sie verfügbar sind.

Einzelheiten zu den neuesten Versionen der AWS Control Tower Account Factory for Terraform (AFT) -Funktionalität finden Sie in der Release-Datei für dieses GitHub Repository.

Voraussetzungen für die Bereitstellung

Bevor Sie Ihre AFT-Umgebung konfigurieren und starten, müssen Sie über die folgenden Ressourcen verfügen:

- Eine Heimatregion für Ihre AWS Control Tower Tower-Landezone. Weitere Informationen finden Sie unter So AWS-Regionen arbeiten Sie mit AWS Control Tower.
- Eine landing zone im AWS Control Tower. Weitere Informationen finden Sie unter Planen Ihrer AWS Control Tower Tower-Landezone.
- Ein AFT-Verwaltungskonto, das Sie in AWS Control Tower oder auf andere Weise bereitstellen und sich bei AWS Control Tower registrieren können.
- Eine Terraform-Version und -Distribution. Weitere Informationen finden Sie unter Terraform - und AFT-Versionen.
- Ein VCS-Anbieter für die Nachverfolgung und Verwaltung von Änderungen an Code und anderen Dateien. Standardmäßig verwendet AWS CodeCommit AFT. Weitere Informationen finden Sie unter Was ist AWS CodeCommit? im AWS CodeCommit Benutzerhandbuch.

  Wenn Sie AFT zum ersten Mal bereitstellen und kein vorhandenes CodeCommit Repository haben, müssen Sie einen externen VCS-Anbieter wie GitHub oder BitBucket wählen. Weitere Informationen finden Sie unter Alternativen zur Versionskontrolle von Quellcode in AFT.
- Eine Laufzeitumgebung, in der Sie das Terraform-Modul ausführen können, das AFT installiert.
- AFT-Funktionsoptionen. Weitere Informationen finden Sie unter Funktionsoptionen aktivieren.

Konfigurieren und starten Sie Ihre AWS Control Tower Account Factory für Terraform

Bei den folgenden Schritten wird davon ausgegangen, dass Sie mit dem Terraform-Workflow vertraut sind. Sie können auch mehr über die Bereitstellung von AFT erfahren, indem Sie dem Lab Einführung in AFT auf der AWS Workshop Studio-Website folgen.

Schritt 1: Starten Sie Ihre AWS Control Tower Tower-Landezone

Anweisungen zu den ersten Schritten mit AWS Control Tower finden Sie unter Erste Schritte mit AWS Control Tower. Hier erstellen Sie das AWS Control Tower Tower-Verwaltungskonto und richten Ihre AWS Control Tower Tower-Landezone ein.

> **Note**
>
> Stellen Sie sicher, dass Sie eine Rolle für das AWS Control Tower Tower-Verwaltungskonto mit AdministratorAccessAnmeldeinformationen erstellen. Weitere Informationen finden Sie hier:
>
> - IAM-Identitäten (Benutzer, Benutzergruppen und Rollen) im AWS Identity and Access Management Benutzerhandbuch
> - AdministratorAccessim Referenzhandbuch für AWS verwaltete Richtlinien

Schritt 2: Erstellen Sie eine neue Organisationseinheit für AFT (dringend empfohlen)

Wir empfehlen Ihnen, eine separate Organisationseinheit in Ihrer AWS Control Tower Tower-Landing landing zone zu erstellen. In dieser Organisationseinheit stellen Sie das AFT-Verwaltungskonto bereit. Erstellen Sie die neue Organisationseinheit und das AFT-Verwaltungskonto von Ihrem AWS Control Tower Tower-Verwaltungskonto aus. Weitere Informationen finden Sie unter Neue Organisationseinheit erstellen.

Schritt 3: Stellen Sie das AFT-Verwaltungskonto bereit

AFT erfordert, dass Sie ein AWS Konto einrichten, das für AFT-Verwaltungsvorgänge vorgesehen ist. Erstellen Sie das AFT-Verwaltungskonto, wenn Sie bei dem AWS Control Tower Tower-Verwaltungskonto angemeldet sind, das Ihrer AWS Control Tower Tower-Landezone zugeordnet ist. Sie können das AFT-Verwaltungskonto von der AWS Control Tower Tower-Konsole aus bereitstellen, indem Sie auf der Seite Organisation die Option Konto erstellen auswählen, oder auf andere Weise. Weitere Informationen finden Sie unter Konten mit AWS Service Catalog Account Factory bereitstellen.

> **Note**
>
> Wenn Sie eine separate OU für AFT erstellt haben, achten Sie darauf, diese OU auszuwählen, wenn Sie das AFT-Verwaltungskonto erstellen.

Es kann bis zu 30 Minuten dauern, bis das AFT-Verwaltungskonto vollständig bereitgestellt ist.

Schritt 4: Stellen Sie sicher, dass die Terraform-Umgebung für die Bereitstellung verfügbar ist

Dieser Schritt setzt voraus, dass Sie Erfahrung mit Terraform haben und über Verfahren zur Ausführung von Terraform verfügen. Weitere Informationen finden Sie unter Command: init auf der Entwickler-Website. HashiCorp

> **Note**
>
> AFT unterstützt die Terraform-Version `1.6.1` oder höher.

Schritt 5: Optionale Konfigurationen

- Legen Sie optional die Virtual Private Cloud (VPC) -Konfiguration fest

  Das AFT-Modul enthält einen `aft_enable_vpc` Parameter, der angibt, ob AWS Control Tower Kontoressourcen innerhalb einer VPC im zentralen AFT-Verwaltungskonto bereitstellt. Standardmäßig ist der Parameter auf `true` eingestellt. Wenn Sie diesen Parameter auf setzen`false`, stellt AWS Control Tower AFT ohne die Verwendung einer VPC und privater Netzwerkressourcen wie NAT-Gateways oder VPC-Endpoints bereit. Die Deaktivierung *`aft_enable_vpc`* kann bei einigen Nutzungsmustern dazu beitragen, die Betriebskosten von AFT zu senken. Das Hinzufügen von VPC-Konfigurationen überschreibt den `aft_enable_vpc` Parameter, auf den gesetzt ist. `false`

  > **Note**
  >
  > Re-enabling Für den `aft_enable_vpc` Parameter (Umschalten des Werts von `false` auf`true`) müssen Sie den `terraform apply` Befehl möglicherweise zweimal hintereinander ausführen.

Anstatt eine neue VPC bereitzustellen, können Sie AFT so konfigurieren, dass eine vorhandene VPC in Ihrem Konto verwendet wird. Um Ihre eigene VPC zu verwenden, geben Sie die folgenden VPC-Konfigurationsparameter an:

- `aft_customer_vpc_id`- Die ID Ihrer bestehenden VPC
- `aft_customer_private_subnets`- Eine Liste der privaten Subnetz-IDs in Ihrer VPC

Beispielkonfiguration:

```
module "aft" {
  source = "github.com/aws-ia/terraform-aws-control_tower_account_factory"

  # VPC configuration
  aft_customer_vpc_id = "vpc-0123456789abcdef0"
  aft_customer_private_subnets = ["subnet-0123456789abcdef0",
 "subnet-0123456789abcdef1"]

  # Other AFT parameters...
}
```

> **Important**
>
> Es wird nicht empfohlen, die benutzerdefinierte VPC-Option zu verwenden, wenn Sie bereits über eine AFT-Bereitstellung verfügen. Möglicherweise sind Sie von Lambda-Funktionen abhängig oder CodePipeline hängen von Ressourcen innerhalb der zugrunde liegenden vorhandenen VPC ab.

- Konfigurieren Sie optional den Terraform-Projektnamen

  Sie können den von AFT verwendeten Terraform-Projektnamen anpassen, indem Sie den Parameter festlegen. `terraform_project_name` Standardmäßig platziert AFT die Bereitstellung im „Standard“ -Projekt in HCP Terraform oder Terraform Enterprise.

  Beispielkonfiguration:

```
module "aft" {
```

```
  source = "github.com/aws-ia/terraform-aws-control_tower_account_factory"

  # Project name configuration
  terraform_project_name = "my-organization-aft"

  # Other AFT parameters...
}
```

> **Note**
>
> Dieser Parameter gilt nur für Terraform Enterprise- oder Terraform Cloud-Bereitstellungen.

- Wenden Sie optional benutzerdefinierte Tags auf AFT-Ressourcen an

  Mithilfe des `tags` Parameters können Sie benutzerdefinierte Tags auf alle AFT-Ressourcen anwenden. Diese Tags helfen bei der Ressourcenorganisation, Kostenzuweisung und Zugriffskontrolle.

  Beispielkonfiguration:

```
module "aft" {
  source = "github.com/aws-ia/terraform-aws-control_tower_account_factory"

  # Custom tags configuration
  tags = {
    Environment = "Production"
    CostCenter = "IT-12345"
    Project = "AFT-Deployment"
    Owner = "platform-team@example.com"
  }

  # Other AFT parameters...
}
```

  Diese Tags werden auf alle Ressourcen angewendet, die vom AFT-Modul erstellt wurden. AFT fügt allen Ressourcen automatisch ein `managed_by = "AFT"` Tag hinzu, das nicht durch benutzerdefinierte Tags überschrieben werden kann.

> **Note**
>
> Benutzerdefinierte Tags können jederzeit hinzugefügt werden, nicht nur bei der ersten Bereitstellung.

- Wenden Sie optional einen AWS KMS vom Kunden verwalteten Verschlüsselungsschlüssel (CMK) auf CloudWatch Protokollgruppen und SNS-Themen an

  Um die KMS-CMK-Verschlüsselung für Protokollgruppen und SNS-Themen zu aktivieren, legen Sie die Variablen und fest. `cloudwatch_log_group_enable_cmk_encryption` `sns_topic_enable_cmk_encryption`

  Wenn Sie sich für diese Einstellungen entscheiden, verwendet AFT das vorhandene CMK, alias/aft, um CloudWatch Protokolle und SNS-Themen zu verschlüsseln. Dieser CMK wird erstellt, wenn AFT im AFT-Verwaltungskonto bereitgestellt wird, und er kann auf Protokollgruppen und SNS-Themen angewendet werden.

  - Wenn die Variable auf true gesetzt `cloudwatch_log_group_enable_cmk_encryption` ist, werden die CloudWatch Protokollgruppen für AFT mit dem CMK verschlüsselt. Wenn die Variable auf False gesetzt ist, was der Standardwert ist, werden die Protokolle mit serverseitiger Verschlüsselung verschlüsselt, wobei die CloudWatch Standardprotokolle verwendet werden.
  - Wenn die Variable auf true gesetzt `sns_topic_enable_cmk_encryption` ist, werden Benachrichtigungen, die an die AFT-SNS-Themen gesendet werden (aft-notifications und aft-failure-notifications), mit dem CMK verschlüsselt. Wenn die Variable auf False gesetzt ist, was der Standardwert ist, werden die SNS-Nachrichten mit dem Schlüssel: /sns verschlüsselt. AWS-managed alias/aws Weitere Informationen finden Sie unter SSE-Schlüsselbegriffe.
- Ändern Sie optional Ihren CodeBuild Rechnertyp

  Um den von AFT verwendeten Berechnungstyp während der Bereitstellung zu ändern CodeBuild, legen Sie die Variable fest`aft_codebuild_compute_type`.

  Informationen zu akzeptierten Berechnungstypen finden Sie unter Über On-Demand-Umgebungstypen. Der Standard-Berechnungstyp ist`BUILD_GENERAL1_MEDIUM`.
- Konfigurieren Sie optional OpenID Connect (OIDC) für Terraform

  Kunden, die Terraform Enterprise oder HCP Terraform (ehemals Terraform Cloud) verwenden, können die Workload-Identitätstoken (oder dynamischen Anbieteranmeldedaten) von Terraform

verwenden, die auf dem OIDC-Protokoll basieren, um Workspaces sicher mit AFT zu verbinden und zu authentifizieren.

Sie können die OIDC-Integration für AFT-Arbeitsbereiche aktivieren, indem Sie den Parameter auf setzen. `terraform_oidc_integration` `true` Dieser Parameter ist standardmäßig auf `false` festgelegt. Wenn Sie diesen Parameter aktivieren, sollten die `terraform_oidc_hostname` Parameter `terraform_oidc_aws_audience` und überprüft und konfiguriert werden`app.terraform.io`, falls die Standardwerte (`aws.workload.identity`bzw.) nicht mit Ihrer Umgebung übereinstimmen.

Beispielkonfiguration:

```
module "aft" {
  source = "github.com/aws-ia/terraform-aws-control_tower_account_factory"

  # Terraform distribution must be "tfc" or "tfe" for OIDC
  terraform_distribution = "tfc"

  # Terraform OIDC Configuration
  terraform_oidc_integration  = true
  terraform_oidc_aws_audience = "aws.workload.identity"  # default
  terraform_oidc_hostname     = "app.terraform.io"       # default; set to your TFE
 hostname if applicable

  # Other AFT parameters...
}
```

> **Note**
>
> Dieser Parameter gilt nur für Terraform Enterprise- oder HCP Terraform-Bereitstellungen.

> **Note**
>
> Wenn Sie derzeit einen OIDC-Anbieter für Terraform im AFT-Verwaltungskonto nutzen, müssen Sie diesen Anbieter löschen, bevor Sie sich für diese Integration anmelden. AFT erstellt diesen Anbieter bei der Bereitstellung für Sie neu.

Schritt 6: Rufen Sie das Account Factory for Terraform-Modul auf, um AFT bereitzustellen

Rufen Sie das AFT-Modul mit der Rolle auf, die Sie für das AWS Control Tower Tower-Verwaltungskonto mit AdministratorAccessAnmeldeinformationen erstellt haben. AWS Control Tower stellt über das AWS Control Tower-Verwaltungskonto ein Terraform-Modul bereit, das die gesamte Infrastruktur einrichtet, die für die Orchestrierung von AWS Control Tower Account Factory Factory-Anfragen erforderlich ist.

Sie können das AFT-Modul im AFT-Repository unter einsehen. GitHub Das gesamte GitHub Repository wird als AFT-Modul betrachtet. In der README-Datei finden Sie Informationen zu den Eingaben, die für die Ausführung des AFT-Moduls und die Bereitstellung von AFT erforderlich sind. Alternativ können Sie das AFT-Modul in der Terraform-Registrierung einsehen.

Wenn Sie in Ihrer Umgebung über Pipelines verfügen, die für die Verwaltung von Terraform eingerichtet wurden, können Sie das AFT-Modul in Ihren bestehenden Workflow integrieren. Andernfalls führen Sie das AFT-Modul in einer beliebigen Umgebung aus, die mit den erforderlichen Anmeldeinformationen authentifiziert wurde.

Ein Timeout führt dazu, dass die Bereitstellung fehlschlägt. Wir empfehlen die Verwendung von AWS -Security-Token-Service (STS-) Anmeldeinformationen, um sicherzustellen, dass Sie einen Timeout haben, der für eine vollständige Bereitstellung ausreicht. Das Mindesttimeout für AWS STS Anmeldeinformationen beträgt 60 Minuten. Weitere Informationen finden Sie unter Temporäre Sicherheitsanmeldeinformationen in IAM im AWS Identity and Access Management Benutzerhandbuch.

> **Note**
>
> Sie können bis zu 30 Minuten warten, bis AFT die Bereitstellung über das Terraform-Modul abgeschlossen hat.

Schritt 7: Verwalten Sie die Terraform-Statusdatei

Bei der Bereitstellung von AFT wird eine Terraform-Statusdatei generiert. Dieses Artefakt beschreibt den Status der Ressourcen, die Terraform erstellt hat. Wenn Sie die AFT-Version aktualisieren möchten, achten Sie darauf, die Terraform-Statusdatei beizubehalten, oder richten Sie ein Terraform-Backend mit Amazon S3 und DynamoDB ein. Das AFT-Modul verwaltet keinen Terraform-Back-End-Status.

> **Note**
>
> Sie sind für den Schutz der Terraform-Statusdatei verantwortlich. Einige Eingabevariablen können sensible Werte enthalten, z. B. einen privaten `ssh` Schlüssel oder ein Terraform-Token. Abhängig von Ihrer Bereitstellungsmethode können diese Werte in der Terraform-Statusdatei als Klartext angezeigt werden. Weitere Informationen finden Sie unter Sensible Daten in State auf der HashiCorp Website.

Post-deployment Schritte

Wenn die Bereitstellung der AFT-Infrastruktur abgeschlossen ist, folgen Sie diesen zusätzlichen Schritten, um den Einrichtungsprozess abzuschließen und sich auf die Bereitstellung von Konten vorzubereiten.

Schritt 1: Schließen Sie den Vorgang AWS CodeConnections mit Ihrem gewünschten VCS-Anbieter ab

Wenn Sie sich für einen VCS-Drittanbieter entscheiden AWS CodeConnections, richtet AFT ihn ein und Sie bestätigen ihn. Weitere Informationen Alternativen zur Versionskontrolle von Quellcode in AFT zur Einrichtung von AFT mit Ihrem bevorzugten VCS finden Sie unter.

Der erste Schritt zum Herstellen der AWS CodeStar Verbindung wird von AFT ausgeführt. Sie müssen die Verbindung bestätigen.

Schritt 2: Füllen Sie jedes Repository aus

AFT erfordert, dass Sie vier Repositorys verwalten:

1. Kontoanfragen — Dieses Repository verarbeitet das Stellen oder Aktualisieren von Kontoanfragen. Verfügbare Beispiele. Weitere Informationen zu AFT-Kontoanfragen finden Sie unterStellen Sie ein neues Konto bei AFT bereit.
2. Anpassungen bei der Bereitstellung von AFT-Konten — Dieses Repository verwaltet Anpassungen, die auf alle Konten angewendet werden, die von AFT erstellt und mit AFT verwaltet werden, bevor mit der Phase der globalen Anpassungen begonnen wird. Verfügbare Beispiele. Informationen zum Erstellen von Anpassungen für die Bereitstellung von AFT-Konten finden Sie unter. Erstellen Sie Ihre Zustandsmaschine für Anpassungen bei der Bereitstellung Ihres AFT-Kontos

3. Globale Anpassungen — Dieses Repository verwaltet Anpassungen, die auf alle Konten angewendet werden, die von AFT erstellt und mit AFT verwaltet werden. Verfügbare Beispiele. Informationen zum Erstellen globaler AFT-Anpassungen finden Sie unterWenden Sie globale Anpassungen an.
4. Kontoanpassungen — Dieses Repository verwaltet Anpassungen, die nur auf bestimmte Konten angewendet werden, die von AFT erstellt und mit AFT verwaltet werden. Verfügbare Beispiele. Informationen zum Erstellen von AFT-Kontoanpassungen finden Sie unterWenden Sie Kontoanpassungen an.

AFT geht davon aus, dass jedes dieser Repositorys einer bestimmten Verzeichnisstruktur folgt. Die Vorlagen, die zum Auffüllen Ihrer Repositorys verwendet werden, und Anweisungen, die beschreiben, wie Sie die Vorlagen füllen, sind im Modul Account Factory for Terraform im AFT-Github-Repository verfügbar.

Stellen Sie ein neues Konto bei AFT bereit

In diesem Abschnitt wird davon ausgegangen, dass Sie AFT und Ihr AFT-Verwaltungskonto bereits eingerichtet haben und zusätzliche Konten bereitstellen.

Um ein neues Konto bei AFT bereitzustellen, erstellen Sie eine Terraform-Datei zur Kontoanforderung. Diese Datei enthält die Eingabe für Parameter im aft-account-request Repository. Nachdem Sie eine Terraform-Datei für Kontoanfragen erstellt haben, beginnen Sie mit der Bearbeitung Ihrer Kontoanfrage, indem Sie Folgendes ausführen. `git push` Dieser Befehl ruft den `ct-aft-account-request` Vorgang in der auf AWS CodePipeline, der nach Abschluss der Kontobereitstellung im AFT-Verwaltungskonto erstellt wird. Weitere Informationen finden Sie unter Pipeline für die Bereitstellung von AFT-Konten.

Terraform-Dateiparameter für Kontoanfragen

Sie müssen die folgenden Parameter in Ihre Terraform-Datei für Kontoanfragen aufnehmen. Ein Beispiel für eine Terraform-Datei zur Kontoanfrage finden Sie unter. GitHub

- Der Wert von `module name` muss für die Anfrage eindeutig sein. AWS-Konto
- Der Wert von `module source` ist der Pfad zum Terraform-Modul für Kontoanfragen, das AFT bereitstellt.
- Der Wert von `control_tower_parameters` erfasst die erforderlichen Eingaben, um ein AWS Control Tower-Konto zu erstellen. Der Wert umfasst die folgenden Eingabefelder:

- `AccountEmail`
- `AccountName`
- `ManagedOrganizationalUnit`
- `SSOUserEmail`
- `SSOUserFirstName`
- `SSOUserLastName`

> **Note**
>
> Die Eingabe, die Sie angeben, `control_tower_parameters` kann während der Kontobereitstellung nicht geändert werden.
> Zu den unterstützten Formaten für die Angabe `ManagedOrganizationalUnit` im aft-account-request Repository gehören und. `OUName` `OUName (OU-ID)` Für verschachtelte Organisationseinheiten (eine Organisationseinheit innerhalb einer Organisationseinheit) müssen Sie das Format verwenden. `OUName (OU-ID)` Ein Beispiel finden Sie unter https://github.com/aws-ia/terraform-aws-control_tower_account_factory/blob/main/sources/aft-customizations-repos/aft-account-request/examples/account-request.tf#L12-L13 account-request.tf in. GitHub

- `account_tags`erfasst benutzerdefinierte Schlüssel und Werte, die nach Geschäftskriterien gekennzeichnet AWS-Konten werden können. Weitere Informationen finden Sie im AWS Organizations Benutzerhandbuch unter Markieren von AWS Organizations Ressourcen.
- Der Wert von `change_management_parameters` erfasst zusätzliche Informationen, z. B. warum eine Kontoanfrage erstellt wurde und wer die Kontoanfrage initiiert hat. Der Wert umfasst die folgenden Eingabefelder:
  - `change_reason`
  - `change_requested_by`
- `custom_fields`erfasst zusätzliche Metadaten mit Schlüsseln und Werten, die als SSM-Parameter im Verkaufskonto unter/aft/account- request/custom -fields/ bereitgestellt werden. Sie können bei Kontoanpassungen auf diese Metadaten verweisen, um die richtigen Steuerelemente bereitzustellen. Beispielsweise könnte ein Konto, das der Einhaltung gesetzlicher Vorschriften unterliegt, zusätzliche AWS-Config-Regeln Dienste bereitstellen. Die Metadaten, die Sie sammeln, `custom_fields` können bei der Kontobereitstellung und -aktualisierung

zusätzliche Verarbeitungsschritte nach sich ziehen. Wenn ein benutzerdefiniertes Feld aus der Kontoanforderung entfernt wird, wird das benutzerdefinierte Feld aus dem SSM-Parameterspeicher für das gekaufte Konto entfernt.

- (Optional) `account_customizations_name` erfasst den Ordner mit den Kontovorlagen im Repository aft-account-customizations. Weitere Informationen finden Sie unter Kontoanpassungen. https://docs.aws.amazon.com/controltower/latest/userguide/aft-account-customization-options.html

Reichen Sie mehrere Kontoanfragen ein

AFT verarbeitet Kontoanfragen einzeln, Sie können jedoch mehrere Kontoanfragen an die AFT-Pipeline senden. Wenn Sie mehrere Kontoanfragen an die AFT-Pipeline senden, stellt AFT die Kontoanfragen in die Warteschlange und verarbeitet sie in der Reihenfolge First-In, First-Out.

> **Note**
>
> Sie können eine Terraform-Datei für Kontoanfragen für jedes Konto erstellen, für das AFT mehrere Kontoanfragen bereitstellen soll, oder mehrere Kontoanfragen in einer einzigen Terraform-Datei für Kontoanfragen kaskadieren.

Aktualisieren Sie ein vorhandenes Konto

> **Kompatibilität mit der automatischen Registrierung**
>
> Wenn Ihre Organisation die automatische Registrierung für die automatische Kontoregistrierung verwendet, beachten Sie, dass AFT beim Import dieser Konten Einschränkungen hat. Konten, die über die automatische Registrierung registriert wurden, verfügen nicht über die vom Service Catalog bereitgestellten Produkte, die für den Import-Workflow von AFT erforderlich sind.
> Problemumgehung: Verwenden Sie die Funktion „Organisationseinheit registrieren“, um bereitgestellte Produkte für automatisch registrierte Konten zu erstellen. Dadurch werden die notwendigen Lebenszyklusereignisse für AFT-Anpassungen aktiviert.

Sie können Konten, die AFT bereitstellt, aktualisieren, indem Sie zuvor eingereichte Kontoanfragen bearbeiten und ausführen`git push`. Dieser Befehl ruft den Workflow zur Kontobereitstellung

auf und kann Anfragen zur Kontoaktualisierung verarbeiten. Sie können die Eingabe für aktualisierenManagedOrganizationalUnit, die Teil des erforderlichen Werts für ist. control_tower_parameters

ManagedOrganizationalUnitist unter allen Parametern der einzige Parameter, der aktualisiert werden kanncontrol_tower_parameters. Andere Parameter, die Teil der Terraform-Datei für Kontoanfragen sind, können jedoch aktualisiert werden, z. B. custom_fields Weitere Informationen finden Sie unter Bereitstellen eines neuen Kontos mit AFT.

Um beispielsweise den Namen oder die E-Mail-Adresse eines AFT-Kontos zu aktualisieren, können Sie die Einzelheiten wie custom_fields in der Kontoanforderungsdatei definieren. Auf diese Weise erstellen Sie SSM-Parameter, die Sie bei globalen Anpassungen an die aws_account_alternate_contact Ressource übergeben können.

```
resource "aws_account_alternate_contact" "operations" {

  alternate_contact_type = "OPERATIONS"

  name          = "Example"
  title         = "Example"
  email_address = "someone@example.com"
  phone_number  = "+1234567890"
}
```

Sie können ähnliche Felder für andere Kontakttypen hinzufügen, z. B. für Betrieb und Sicherheit. Fügen Sie unter Globale Anpassungen Datenabfragen für jedes benutzerdefinierte Feld hinzu, um sicherzustellen, dass Sie alle Felder nachschlagen, die Sie in der Kontoanfrage erstellt haben:

```
data "aws_ssm_parameter" "billing_name" {
            name = "/aft/account-request/custom-fields/billing_name"
            }

            data "aws_ssm_parameter" "billing_title" {
            name = "/aft/account-request/custom-fields/billing_title"
            }

            data "aws_ssm_parameter" "billing_email_address" {
            name = "/aft/account-request/custom-fields/billing_email_address"
            }

            data "aws_ssm_parameter" "billing_phone_number" {
```

```
            name = "/aft/account-request/custom-fields/billing_phone_number"
            }
```

Erstellen Sie abschließend ebenfalls in der Datei mit den globalen Anpassungen die alternativen Kontaktressourcen. Sie müssen einen dieser Blöcke für jeden Kontakttyp definieren, den Sie in der Kontoanfrage erstellt haben:

```
resource "aws_account_alternate_contact" "billing" {

            alternate_contact_type = "BILLING"

            name          = data.aws_ssm_parameter.billing_name.value
            title         = data.aws_ssm_parameter.billing_title.value
            email_address = data.aws_ssm_parameter.billing_email_address.value
            phone_number  = data.aws_ssm_parameter.billing_phone_number.value
            }
```

> **Note**
>
> Die von Ihnen bereitgestellten Eingaben `control_tower_parameters` können bei der Kontobereitstellung nicht geändert werden.
> Zu den unterstützten Formaten für die Angabe `ManagedOrganizationalUnit` im aft-account-request Repository gehören und. `OUName` `OUName (OU-ID)` Für verschachtelte Organisationseinheiten (eine Organisationseinheit innerhalb einer Organisationseinheit) müssen Sie das Format verwenden. `OUName (OU-ID)` Ein Beispiel finden Sie unter https://github.com/aws-ia/terraform-aws-control_tower_account_factory/blob/main/sources/aft-customizations-repos/aft-account-request/examples/account-request.tf#L12-L13 account-request.tf in. GitHub

Aktualisieren Sie ein Konto, das AFT nicht bereitstellt

Sie können AWS Control Tower-Konten, die außerhalb von AFT erstellt wurden, aktualisieren, indem Sie das Konto im aft-account-request Repository angeben.

> **Note**
>
> Stellen Sie sicher, dass alle Kontoinformationen korrekt sind und mit der AWS Control Tower-Organisation und dem jeweiligen bereitgestellten Produkt übereinstimmen. AWS Service Catalog

Voraussetzungen für die Aktualisierung eines bestehenden AWS-Konto mit AFT

- Der AWS-Konto muss bei AWS Control Tower registriert sein.
- Der AWS-Konto muss Teil der AWS Control Tower-Organisation sein.

Terraform- und AFT-Versionen

Account Factory for Terraform (AFT) unterstützt die Terraform-Version oder höher. `1.6.1` Sie müssen eine Terraform-Version als Eingabeparameter für den AFT-Bereitstellungsprozess angeben, wie im folgenden Beispiel gezeigt.

```
terraform_version = "1.6.1"
```

Terraform-Verteilungen

AFT unterstützt drei Terraform-Verteilungen:

- Terraform Community Edition
- HCP Terraform
- Terraform Enterprise

Diese Verteilungen werden in den folgenden Abschnitten erklärt. Geben Sie während des AFT-Bootstrap-Prozesses die Terraform-Verteilung Ihrer Wahl als Eingabeparameter an. Weitere Informationen zur AFT-Bereitstellung und zu Eingabeparametern finden Sie unter. Stellen Sie AWS Control Tower Account Factory für Terraform (AFT) bereit

Wenn Sie sich für die HCP Terraform- oder Terraform Enterprise-Distributionen entscheiden, `terraform_token` muss es sich bei dem API-Token, für das Sie angeben, um ein Benutzer- oder Team-API-Token handeln. Ein Organisationstoken wird nicht für alle erforderlichen APIs unterstützt. Aus Sicherheitsgründen müssen Sie vermeiden, den Wert dieses Tokens in Ihr

Versionskontrollsystem (VCS) einzuchecken, indem Sie eine Terraform-Variable zuweisen, wie im folgenden Beispiel gezeigt.

```
# Sensitive variable managed in HCP Terraform:
terraform_token = var.terraform_cloud_token
```

Terraform Community Edition

Wenn Sie Terraform Community Edition als Distribution auswählen, verwaltet AFT das Terraform-Backend für Sie im AFT-Verwaltungskonto. AFT lädt die `terraform-cli` von Ihnen angegebene Terraform-Version herunter, um sie während der AFT-Bereitstellung und der AFT-Pipeline-Phase auszuführen. Die resultierende Terraform-State-Konfiguration wird in einem Amazon S3 S3-Bucket gespeichert, der in der folgenden Form benannt ist:

```
aft-backend-[account_id]-primary-region
```

AFT erstellt außerdem einen Amazon S3 S3-Bucket, der Ihre Terraform-Zustandskonfiguration zu Notfallwiederherstellungszwecken in einem anderen AWS-Region repliziert und in der folgenden Form benannt ist:

```
aft-backend-[account_id]-secondary-region
```

Wir empfehlen, die Multi-Faktor-Authentifizierung (MFA) für Löschfunktionen in diesen Amazon S3 S3-Buckets im Terraform-Status zu aktivieren. Weitere Informationen zur Terraform Community Edition finden Sie in der Terraform-Dokumentation.

Um Terraform OSS als Ihre Distribution auszuwählen, geben Sie den folgenden Eingabeparameter an:

```
terraform_distribution = "oss"
```

HCP Terraform

Wenn Sie HCP Terraform als Distribution auswählen, erstellt AFT Workspaces für die folgenden Komponenten in Ihrer HCP Terraform-Organisation, wodurch ein Workflow initiiert wird. API-driven

- Kontoanfrage
- AFT-Anpassungen für Konten, die von AFT bereitgestellt werden

- Kontoanpassungen für Konten, die von AFT bereitgestellt werden
- Globale Anpassungen für Konten, die von AFT bereitgestellt werden

HCP Terraform verwaltet die resultierende Terraform-State-Konfiguration.

Wenn Sie HCP Terraform als Ihre Distribution auswählen, geben Sie die folgenden Eingabeparameter an:

- `terraform_distribution = "tfc"`
- `terraform_token`— Dieser Parameter enthält den Wert des HCP Terraform-Tokens. AFT markiert den als sensibel und speichert den Wert als sichere Zeichenfolge im SSM-Parameterspeicher des AFT-Verwaltungskontos. Wir empfehlen Ihnen, den Wert des Terraform-Tokens regelmäßig entsprechend den Sicherheits- und Compliance-Richtlinien Ihres Unternehmens zu ändern. Das Terraform-Token sollte ein API-Token auf Benutzer- oder Teamebene sein. Organisationstoken werden nicht unterstützt.
- `terraform_org_name`— Dieser Parameter enthält den Namen Ihrer HCP Terraform-Organisation.

> **Note**
>
> Mehrere AFT-Bereitstellungen in einer einzigen HCP Terraform-Organisation werden nicht unterstützt.

Informationen zur Einrichtung von HCP Terraform finden Sie in der Terraform-Dokumentation.

Terraform Enterprise

Wenn Sie Terraform Enterprise als Distribution auswählen, erstellt AFT Arbeitsbereiche für die folgenden Komponenten in Ihrer Terraform Enterprise-Organisation und löst API-driven den Workflow für die resultierenden Terraform-Läufe aus.

- Kontoanfrage
- Anpassungen der AFT-Kontobereitstellung für von AFT bereitgestellte Konten
- Kontoanpassungen für von AFT bereitgestellte Konten
- Globale Anpassungen für von AFT bereitgestellte Konten

Die resultierende Terraform-State-Konfiguration wird von Ihrem Terraform Enterprise-Setup verwaltet.

Um Terraform Enterprise als Ihre Distribution auszuwählen, geben Sie die folgenden Eingabeparameter an:

- `terraform_distribution = "tfe"`
- `terraform_token`— Dieser Parameter enthält den Wert Ihres Terraform Enterprise-Tokens. AFT markiert seinen Wert als sensibel und speichert ihn als sichere Zeichenfolge im SSM-Parameterspeicher im AFT-Verwaltungskonto. Wir empfehlen, dass Sie den Wert des Terraform-Tokens regelmäßig entsprechend den Sicherheits- und Compliance-Richtlinien Ihres Unternehmens ändern.
- `terraform_org_name`— Dieser Parameter enthält den Namen Ihrer Terraform Enterprise-Organisation.
- `terraform_api_endpoint`— Dieser Parameter enthält die URL Ihrer Terraform Enterprise-Umgebung. Der Wert dieses Parameters muss das folgende Format haben:

```
https://{fqdn}/api/v2/
```

Weitere Informationen zur Einrichtung von Terraform Enterprise finden Sie in der Terraform-Dokumentation.

Überprüfen Sie die AFT-Version

Sie können Ihre bereitgestellte AFT-Version überprüfen, indem Sie den AWS SSM Parameter Store-Schlüssel abfragen:

```
/aft/config/aft/version
```

Wenn Sie die Registrierungsmethode verwenden, können Sie die Version anheften.

```
module "control_tower_account_factory" {
  source  = "aws-ia/control_tower_account_factory/aws"
  version = "1.3.2"
  # insert the 6 required variables here
}
```

Weitere Informationen zu AFT-Versionen finden Sie im AFT-Repository.

Aktualisieren Sie die AFT-Version

Melden Sie sich beim AWS Control Tower Tower-Managementkonto an, um dieses AFT-Update zu initiieren.

Sie können Ihre bereitgestellte AFT-Version aktualisieren, indem Sie sie aus dem `main` Repository-Zweig abrufen:

```
terraform get -update
```

Nachdem der Abruf abgeschlossen ist, können Sie den Terraform-Plan erneut ausführen oder apply ausführen, um die AFT-Infrastruktur mit den neuesten Änderungen zu aktualisieren.

Funktionsoptionen aktivieren

AFT bietet Funktionsoptionen, die auf bewährten Verfahren basieren. Sie können sich während der AFT-Bereitstellung mithilfe von Feature-Flags für diese Funktionen entscheiden. Stellen Sie ein neues Konto bei AFT bereitWeitere Informationen zu den AFT-Eingangskonfigurationsparametern finden Sie unter.

Diese Funktionen sind standardmäßig nicht aktiviert. Sie müssen jede Funktion in Ihrer Umgebung explizit aktivieren.

Themen

- AWS CloudTrail Datenereignisse
- AWS Support-Plan für Unternehmen
- Löschen Sie die AWS Standard-VPC
- Exportieren Sie die Terraform-Planausgabe nach Amazon S3

AWS CloudTrail Datenereignisse

Wenn diese Option aktiviert ist, konfiguriert die Option für AWS CloudTrail Datenereignisse diese Funktionen.

- Erstellt einen Organization Trail im AWS Control Tower Tower-Managementkonto, für CloudTrail
- Aktiviert die Protokollierung für Amazon S3- und Lambda-Datenereignisse
- Verschlüsselt und exportiert alle CloudTrail Datenereignisse mit AWS KMS Verschlüsselung in einen `aws-aft-logs-*` S3-Bucket im AWS Control Tower Log Archive-Konto

- Aktiviert die Einstellung zur Überprüfung der Protokolldatei

Um diese Option zu aktivieren, setzen Sie das folgende Feature-Flag in Ihrer AFT-Bereitstellungs-Eingabekonfiguration auf True.

```
aft_feature_cloudtrail_data_events
```

Voraussetzung

Bevor Sie diese Funktionsoption aktivieren, stellen Sie sicher, dass der vertrauenswürdige Zugriff für in Ihrer Organisation aktiviert AWS CloudTrail ist.

So überprüfen Sie den Status des vertrauenswürdigen Zugriffs für CloudTrail :

1. Navigieren Sie zur AWS Organizations Konsole.
2. Wählen Sie Dienste > CloudTrail.
3. Wählen Sie dann bei Bedarf oben rechts die Option Vertrauenswürdigen Zugriff aktivieren aus.

Möglicherweise erhalten Sie eine Warnmeldung, in der Sie aufgefordert werden, die AWS CloudTrail Konsole zu verwenden. In diesem Fall sollten Sie die Warnung jedoch ignorieren. AFT erstellt den Trail im Rahmen der Aktivierung dieser Funktionsoption, nachdem Sie den vertrauenswürdigen Zugriff zugelassen haben. Wenn der vertrauenswürdige Zugriff nicht aktiviert ist, erhalten Sie eine Fehlermeldung, wenn AFT versucht, Ihren Trail für Datenereignisse zu erstellen.

> **Note**
>
> Diese Einstellung funktioniert auf Organisationsebene. Die Aktivierung dieser Einstellung wirkt sich auf alle Konten in aus AWS Organizations, unabhängig davon, ob sie von AFT verwaltet werden oder nicht. Alle Buckets im AWS Control Tower Log Archive-Konto zum Zeitpunkt der Aktivierung sind von Amazon S3 S3-Datenereignissen ausgeschlossen. Weitere Informationen zu finden Sie im AWS CloudTrail Benutzerhandbuch. CloudTrail

AWS Support-Plan für Unternehmen

Wenn diese Option aktiviert ist, aktiviert die AFT-Pipeline den AWS Enterprise Support-Plan für von AFT bereitgestellte Konten.

AWS Bei Konten ist standardmäßig der AWS Basic Support-Plan aktiviert. AFT bietet für Konten, die von AFT bereitgestellt werden, eine automatische Registrierung für die Enterprise-Support-Stufe. Der Bereitstellungsprozess öffnet ein Support-Ticket für das Konto und fordert auf, es zum AWS Enterprise Support-Plan hinzuzufügen.

Um die Enterprise Support-Option zu aktivieren, setzen Sie das folgende Feature-Flag in Ihrer AFT-Bereitstellungs-Eingabekonfiguration auf True.

```
aft_feature_enterprise_support=false
```

Weitere Informationen zu AWS Supportplänen finden Sie unter AWS Supportpläne vergleichen.

> **Note**
>
> Damit diese Funktion funktionieren kann, müssen Sie das Zahlerkonto für den Enterprise Support-Plan registrieren.

Löschen Sie die AWS Standard-VPC

Wenn Sie diese Option aktivieren, löscht AFT alle AWS Standard-VPCs im AFT-Verwaltungskonto und insgesamt AWS-Regionen, auch wenn dort keine AWS Control Tower Tower-Ressourcen bereitgestellt wurden. AWS-Regionen

AFT löscht AWS Standard-VPCs nicht automatisch für AWS Control Tower-Konten, die AFT bereitstellt, oder für bestehende AWS Konten, die Sie über AFT bei AWS Control Tower registrieren.

Neue AWS Konten werden standardmäßig mit jeweils AWS-Region einer VPC erstellt. In Ihrem Unternehmen gibt es möglicherweise Standardverfahren für die Erstellung von VPCs, bei denen Sie die AWS Standard-VPC löschen und vermeiden müssen, sie zu aktivieren, insbesondere für das AFT-Verwaltungskonto.

Um diese Option zu aktivieren, setzen Sie das folgende Feature-Flag in Ihrer AFT-Bereitstellungs-Eingabekonfiguration auf True.

```
aft_feature_delete_default_vpcs_enabled
```

Im Folgenden finden Sie ein Beispiel für eine Eingabekonfiguration für die AFT-Bereitstellung.

```
module "aft" {
```

```
  source = "github.com/aws-ia/terraform-aws-control_tower_account_factory"
  ct_management_account_id    = var.ct_management_account_id
  log_archive_account_id      = var.log_archive_account_id
  audit_account_id            = var.audit_account_id
  aft_management_account_id   = var.aft_management_account_id
  ct_home_region              = var.ct_home_region
  tf_backend_secondary_region = var.tf_backend_secondary_region

  vcs_provider                                = "github"
  account_request_repo_name                   = "${var.github_username}/learn-
terraform-aft-account-request"
  account_provisioning_customizations_repo_name = "${var.github_username}/learn-
terraform-aft-account-provisioning-customizations"
  global_customizations_repo_name             = "${var.github_username}/learn-
terraform-aft-global-customizations"
  account_customizations_repo_name            = "${var.github_username}/learn-
terraform-aft-account-customizations"

  # Optional Feature Flags
  aft_feature_delete_default_vpcs_enabled = true
  aft_feature_cloudtrail_data_events      = false
  aft_feature_enterprise_support          = false
}
```

Weitere Informationen zu Standard-VPCs finden Sie unter Standard-VPC und Standard-Subnetze.

> **Note**
>
> Die standardmäßige VPC-Löschung erfolgt nach bestem Bemühen. AWS-Region Wenn der Endpunkt einer Region vorübergehend nicht erreichbar ist, überspringt AFT diese Region und setzt das Löschen von Standard-VPCs in den verbleibenden Regionen fort. Übersprungene Regionen werden beim nächsten Lauf der Anpassungspipeline erneut versucht. Um zu überprüfen, ob Regionen übersprungen wurden, durchsuchen Sie die `aft-delete-default-vpc` Lambda-Funktionsprotokolle nach der Nachricht. `Skipping default VPC deletion in region`

Exportieren Sie die Terraform-Planausgabe nach Amazon S3

Wenn Sie AFT bereitstellen, erstellt AFT einen dedizierten, verschlüsselten Amazon S3 S3-Bucket für die Planausgabe im AFT-Verwaltungskonto. AFT erstellt diesen Bucket bei jeder AFT-

Bereitstellung, unabhängig von Ihrer Terraform-Distribution. Der Bucket speichert die JSON-Ausgabe von Anpassungsläufen, die nur für den Plan vorgesehen sind. Weitere Informationen zu Ausführungen, die nur mit dem Plan ausgeführt werden, finden Sie unter. Re-invoke Anpassungen

Der Plan-Output-Bucket hat die folgenden Eigenschaften:

- Mit dem AFT-Schlüssel verschlüsselt AWS KMS
- Versionierung aktiviert
- Öffentlicher Zugriff gesperrt
- Der Schreibzugriff ist auf die Build-Rolle für AFT-Anpassungen beschränkt

Ob AFT den Plan-JSON in diesen Bucket exportiert, hängt von Ihrer Terraform-Verteilung ab:

- Community Edition (Open Source): AFT exportiert den Plan-JSON standardmäßig bei jeder Ausführung, die nur für den Plan gilt, in den Bucket.
- HCP Terraform (Terraform Cloud) und Terraform Enterprise: Sie können die Planergebnisse in der HCP Terraform Run-Benutzeroberfläche anzeigen. Um auch den Plan-JSON in den Bucket zu exportieren, setzen Sie die folgende Variable in Ihrer Eingabekonfiguration für die AFT-Bereitstellung auf. `true`

```
aft_plan_output_export_enabled = true
```

AFT bewahrt exportierte Pläne standardmäßig 30 Tage lang auf. Um die Aufbewahrungsdauer zu ändern, legen Sie die `aft_plan_output_retention_days` Variable in Ihrer Eingabekonfiguration für die AFT-Bereitstellung fest.

```
aft_plan_output_retention_days = 30
```

> **Note**
>
> Die `aft_plan_output_export_enabled` Variable wirkt sich nur auf die Distributionen HCP Terraform (Terraform Cloud) und Terraform Enterprise aus. In der Community Edition-Distribution (Open Source) exportiert AFT standardmäßig den Plan-JSON, und diese Variable hat keine Auswirkung.

Überlegungen zu Ressourcen für AWS Control Tower Account Factory für Terraform

Wenn Sie Ihre landing zone mit AWS Control Tower Account Factory for Terraform einrichten, werden in Ihren AWS Konten verschiedene Arten von AWS Ressourcen erstellt.

Suchen Sie nach Ressourcen

- Sie können Tags verwenden, um nach der aktuellsten Liste von AFT-Ressourcen zu suchen. Das Schlüssel-Wert-Paar für Ihre Suche ist:

```
Key: managed_by | Value: AFT
```

- Für Komponentendienste, die keine Tags unterstützen, können Sie nach Ressourcen suchen, indem Sie `aft` in den Ressourcennamen nach suchen.

> **Note**
>
> AFT erstellt keine AWS Backup-Ressourcen im Verwaltungskonto.

Tabellen der ursprünglich erstellten Ressourcen, sortiert nach Konten

Verwaltungskonto AWS Control Tower Account Factory für Terraform

AWS Service nicht zulässig	Ressourcentyp	Ressourcenname
AWS Identity and Access Management	Rollen	AWSAFTAdmin
		AWSAFTExecution
		AWSAFTService
		ct-aft-*
		aft-*
		codebuild_trigger_role

AWS Service nicht zulässig	Ressourcentyp	Ressourcenname
		python-layer-builder-aft-common-*
AWS Identity and Access Management	Richtlinien	aft-*
CodeCommit	Repositorien	aft-*
CodeBuild	Build-Projekte	aft-* ct-aft-* python-layer-builder-aft-common-*
Code-Pipeline	Pipelines	*YourAccountId* -customizations-pipeline
Amazon S3	Buckets	aft-*
Amazon S3	Buckets	aft-plan-output-*
Lambda	Funktionen	aft-*
Lambda	Layer	aft-common-*
DynamoDB	Tabellen	aft-request aft-request-audit aft-request-metadata aft-controltower-events

AWS Service nicht zulässig	Ressourcentyp	Ressourcenname
Step Functions	Staatsmaschinen	aft-account-provisioning-customizations aft-account-provisioning-framework aft-feature-options aft-invoke-customizations
VPC	VPC	aft-management-vpc
Amazon SNS	Topics	aft-notifications aft-failure-notifications
Amazon EventBridge	Event Buses	aft-events-from-ct-management
Amazon EventBridge	Regeln für Veranstaltungen	aft-account-provisioning-customizations-trigger aft-account-request-codepipeline-trigger aft-lambda-account-request-processor aft-controltower-event-logger
Schlüsselverwaltungsdienst (KMS)	Vom Kunden verwaltete Schlüssel	aft-backend-*-kms-key aft
AWS Systems Manager	Parameter speichern	/aft/*
Amazon SQS	Queues (Warteschlangen)	aft-account-request.fifo aft-account-request-dlg.fifo

AWS Service nicht zulässig	Ressourcentyp	Ressourcenname
CloudWatch	Protokollgruppen	/aws/*/ct-aft-* /aws/*/aft-* /aws/codebuild/python-layer-builder-aft-common-*
AWS Backup	Tresore	aft-controltower-backup-vault
AWS Backup	Plans (Pläne)	aft-controltower-backup-plan
AWS Kundendienstzentrum (optional)	Unterstützungspläne	Enterprise

AWS Konten, die über AWS Control Tower Account Factory für Terraform bereitgestellt werden

AWS Service nicht zulässig	Ressourcentyp	Ressourcenname
AWS Identity and Access Management	Rollen	AWSAFTExecution
AWS Kundendienstzentrum (optional)	Unterstützungspläne	Enterprise

AWS Control Tower Tower-Verwaltungskonto

AWS Service nicht zulässig	Ressourcentyp	Ressourcenname
AWS Identity and Access Management	Rollen	AWSAFTExecution AWSAFTService aft-controltower-events-rule
AWS Systems Manager	Parameter speichern	/aft/*
EventBridge	Regeln für Veranstaltungen	aft-capture-ct-events

AWS Service nicht zulässig	Ressourcentyp	Ressourcenname
CloudTrail (Fakultativ)	Trails	aws-aft-CustomizationsCloud Trail
AWS-Supportcenter (optional)	Unterstützungspläne	Enterprise

AWS Control Tower Tower-Protokollarchiv-Konto

AWS Service nicht zulässig	Ressourcentyp	Ressourcenname
AWS Identity and Access Management	Rollen	AWSAFTExecution AWSAFTService
Schlüsselverwaltungsservice (KMS)	Vom Kunden verwaltete Schlüssel	aft
Amazon S3	Buckets	aws-aft-logs-* aws-aft-s3-access-logs-*
AWS Kundendienstzentrum (optional)	Unterstützungspläne	Enterprise

AWS Control Tower Tower-Auditkonto

AWS Service nicht zulässig	Ressourcentyp	Ressourcenname
AWS Identity and Access Management	Rollen	AWSAFTExecution AWSAFTService
AWS Kundendienstzentrum (optional)	Unterstützungspläne	Enterprise

Erforderliche Rollen

Im Allgemeinen sind Rollen und Richtlinien Teil des Identitäts- und Zugriffsmanagements (IAM) in. AWS Weitere Informationen finden Sie im AWS IAM-Benutzerhandbuch .

AFT erstellt mehrere IAM-Rollen und -Richtlinien in den AFT-Management- und AWS Control Tower-Managementkonten, um den Betrieb der AFT-Pipeline zu unterstützen. Diese Rollen werden auf der Grundlage des Modells mit den geringsten Rechten erstellt, das die Berechtigungen auf die minimal erforderlichen Aktionen und Ressourcen für jede Rolle und Richtlinie beschränkt. Diesen Rollen und Richtlinien wird zur Identifizierung ein AWS `key:value` Tag-Paar zugewiesen. `managed_by:AFT`

Neben diesen IAM-Rollen erstellt AFT drei wichtige Rollen:

- die Rolle `AWSAFTAdmin`
- die `AWSAFTExecution` Rolle
- die `AWSAFTService` Rolle

Diese Rollen werden in den folgenden Abschnitten erklärt.

Die Rolle AWSaftAdmin, erklärt

Wenn Sie AFT bereitstellen, wird die `AWSAFTAdmin` Rolle im AFT-Verwaltungskonto erstellt. Diese Rolle ermöglicht es der AFT-Pipeline, die `AWSAFTExecution` Rolle in von AWS Control Tower und von AFT bereitgestellten Konten zu übernehmen und so Aktionen im Zusammenhang mit der Kontobereitstellung und Anpassungen durchzuführen.

Hier ist die Inline-Richtlinie (JSON-Artefakt), die der Rolle zugeordnet ist: `AWSAFTAdmin`

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "sts:AssumeRole",
            "Resource": [
                "arn:aws:iam::*:role/AWSAFTExecution",
                "arn:aws:iam::*:role/AWSAFTService"
            ]
```

```
        }
    ]
}
```

Das folgende JSON-Artefakt zeigt die Vertrauensbeziehung für die `AWSAFTAdmin` Rolle. Die Platzhalternummer `012345678901` wird durch die ID-Nummer des AFT-Verwaltungskontos ersetzt.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::012345678901:root"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Die Rolle AWSaftExecution, erklärt

Wenn Sie AFT bereitstellen, wird die `AWSAFTExecution` Rolle in den Verwaltungskonten AFT und AWS Control Tower erstellt. Später erstellt die AFT-Pipeline die `AWSAFTExecution` Rolle in jedem von AFT bereitgestellten Konto während der Bereitstellungsphase des AFT-Kontos.

AFT verwendet die `AWSControlTowerExecution` Rolle zunächst, um die `AWSAFTExecution` Rolle in bestimmten Konten zu erstellen. Die `AWSAFTExecution` Rolle ermöglicht es der AFT-Pipeline, die Schritte auszuführen, die während der Bereitstellungs- und Anpassungsphasen des AFT-Frameworks für von AFT bereitgestellte Konten und für gemeinsam genutzte Konten ausgeführt werden.

> **Verschiedene Rollen helfen Ihnen dabei, den Umfang einzuschränken**
>
> Es hat sich bewährt, die Anpassungsberechtigungen von den Berechtigungen zu trennen, die Ihnen bei der ersten Bereitstellung von Ressourcen gewährt wurden. Denken Sie daran, dass die `AWSAFTService` Rolle für die Kontobereitstellung und die `AWSAFTExecution`

Rolle für die Kontoanpassung vorgesehen ist. Diese Trennung begrenzt den Umfang der Berechtigungen, die in jeder Phase der Pipeline zulässig sind. Diese Unterscheidung ist besonders wichtig, wenn Sie die gemeinsamen Konten im AWS Control Tower anpassen, da die gemeinsamen Konten vertrauliche Informationen wie Rechnungsdetails oder Benutzerinformationen enthalten können.

Berechtigungen für die `AWSAFTExecution` Rolle: AdministratorAccess — eine von AWS verwaltete Richtlinie

Das folgende JSON-Artefakt zeigt die der Rolle zugeordnete IAM-Richtlinie (Vertrauensbeziehung). `AWSAFTExecution` Die Platzhalternummer `012345678901` wird durch die ID-Nummer des AFT-Verwaltungskontos ersetzt.

Vertrauensrichtlinie für `AWSAFTExecution`

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::012345678901:role/AWSAFTAdmin"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Die Rolle AWSaftService, erklärt

Die `AWSAFTService` Rolle stellt AFT-Ressourcen auf allen registrierten und verwalteten Konten bereit, einschließlich der gemeinsamen Konten und des Verwaltungskontos. Ressourcen wurden früher nur von der `AWSAFTExecution` Rolle bereitgestellt.

Die `AWSAFTService` Rolle ist für die Verwendung durch die Dienstinfrastruktur zur Bereitstellung von Ressourcen während der Bereitstellungsphase vorgesehen, und die `AWSAFTExecution` Rolle

ist nur für die Bereitstellung von Anpassungen vorgesehen. Wenn Sie die Rollen auf diese Weise übernehmen, können Sie in jeder Phase eine detailliertere Zugriffskontrolle gewährleisten.

Berechtigungen für die `AWSAFTService` Rolle: AdministratorAccess — eine von AWS verwaltete Richtlinie

Das folgende JSON-Artefakt zeigt die der Rolle zugeordnete IAM-Richtlinie (Vertrauensbeziehung). `AWSAFTService` Die Platzhalternummer `012345678901` wird durch die ID-Nummer des AFT-Verwaltungskontos ersetzt.

Vertrauensrichtlinie für `AWSAFTService`

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::012345678901:role/AWSAFTAdmin"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Komponentendienste

Wenn Sie AFT bereitstellen, werden Ihrer AWS Umgebung von jedem dieser AWS Dienste Komponenten hinzugefügt.

- AWS Control Tower — AFT verwendet AWS Control Tower Account Factory im AWS Control Tower-Verwaltungskonto, um Konten bereitzustellen.
- Amazon DynamoDB — AFT erstellt Amazon DynamoDB-Tabellen im AFT-Verwaltungskonto, in denen Kontoanfragen, der Prüfverlauf von Kontoaktualisierungen, Kontometadaten und AWS Control Tower-Lebenszyklusereignisse gespeichert werden. AFT erstellt auch DynamoDB-Lambda-Trigger, um nachgelagerte Prozesse einzuleiten, z. B. das Starten des Workflows zur Bereitstellung von AFT-Konten.

- Amazon Simple Storage Service — AFT erstellt Amazon Simple Storage Service (S3) -Buckets im AFT-Verwaltungskonto und im AWS Control Tower-Protokollarchivkonto, in denen Protokolle gespeichert werden, die von den AWS Diensten generiert wurden, die die AFT-Pipeline benötigt. AFT erstellt außerdem einen Terraform-Backend-S3-Bucket (primär und sekundär), um Terraform-Status zu speichern AWS-Regionen, die während der AFT-Pipeline-Workflows generiert wurden.
- Amazon Simple Notification Service — AFT erstellt Amazon Simple Notification Service (SNS) -Themen im AFT-Verwaltungskonto, das Erfolgs- und Fehlerbenachrichtigungen nach der Bearbeitung jeder AFT-Kontoanfrage speichert. Möglicherweise erhalten Sie diese Nachrichten mit dem Protokoll Ihrer Wahl.
- Amazon Simple Queuing Service — AFT erstellt eine FIFO-Warteschlange für Amazon Simple Queuing Service (Amazon SQS) im AFT-Verwaltungskonto. Die Warteschlange ermöglicht es Ihnen, mehrere Kontoanfragen parallel einzureichen, aber sie sendet jeweils eine Anfrage zur sequentiellen Verarbeitung an AWS Control Tower Account Factory.
- AWS CodeBuild — AFT erstellt CodeBuild AWS-Build-Projekte im AFT-Verwaltungskonto, um Terraform-Pläne für den AFT-Quellcode in verschiedenen Build-Phasen zu initialisieren, zu kompilieren, zu testen und anzuwenden.
- AWS CodePipeline — AFT erstellt CodePipeline AWS-Pipelines im AFT-Verwaltungskonto, um sie mit Ihrem ausgewählten, unterstützten CodeStar AWS-Verbindungsanbieter für AFT-Quellcode zu integrieren und Build-Jobs in AWS auszulösen. CodeBuild
- AWS Lambda — AFT erstellt AWS-Lambda-Funktionen und -Layer im AFT-Verwaltungskonto, um Schritte während der Kontoanforderung, der AFT-Kontobereitstellung und der Kontoanpassungen durchzuführen.
- AWS Systems Manager Parameter Store — AFT richtet den AWS Systems Manager Parameter Store im AFT-Verwaltungskonto ein, um die für die AFT-Pipeline-Prozesse erforderlichen Konfigurationsparameter zu speichern.
- Amazon CloudWatch — AFT erstellt CloudWatch Amazon-Protokollgruppen im AFT-Verwaltungskonto, um Protokolle zu speichern, die von AWS-Services generiert wurden, die von der AFT-Pipeline verwendet werden. Die Aufbewahrungsfrist für CloudWatch Protokolle ist auf festgelegt`Never Expire`.
- Amazon VPC — AFT erstellt eine Amazon Virtual Private Cloud (VPC), um Dienste und Ressourcen im AFT-Verwaltungskonto in einer separaten Netzwerkumgebung zu isolieren und so die Sicherheit zu erhöhen.
- AWS KMS — AFT verwendet den AWS Key Management Service (KMS) im AFT-Verwaltungskonto und im AWS Control Tower-Protokollarchivkonto. AFT erstellt Schlüssel zum Verschlüsseln von Terraform-Zuständen, in DynamoDB-Tabellen gespeicherten Daten und SNS-

Themen. Diese Protokolle und Artefakte werden generiert, wenn AWS-Ressourcen und -Services von AFT bereitgestellt werden. Bei KMS-Schlüsseln, die von AFT erstellt wurden, ist die jährliche Rotation standardmäßig aktiviert.

- AWS Identitäts- und Zugriffsmanagement (IAM) — AFT folgt dem empfohlenen Least-Privilege-Modell. Es erstellt je nach Bedarf Rollen und Richtlinien für das AWS Identitäts- und Zugriffsmanagement (IAM) im AFT-Verwaltungskonto, in AWS Control Tower-Konten und in von AFT bereitgestellten Konten, um die während des AFT-Pipeline-Workflows erforderlichen Aktionen auszuführen.
- AWS Step Functions — AFT erstellt AWS Step Functions-Zustandsautomaten im AFT-Verwaltungskonto. Diese Zustandsautomaten orchestrieren und automatisieren den Prozess und die Schritte für das Framework zur Bereitstellung von AFT-Konten und die Anpassungen.
- Amazon EventBridge — AFT erstellt einen EventBridge Amazon-Event-Bus im AFT- und AWS Control Tower-Verwaltungskonto, um AWS-Control-Tower-Lebenszyklusereignisse zu erfassen und langfristig in der DynamoDB-Tabelle des AFT-Verwaltungskontos zu speichern. AFT erstellt CloudWatch Amazon-Eventregeln in den AFT-Verwaltungskonten und AWS Control Tower-Verwaltungskonten, die mehrere Schritte auslösen, die während der Ausführung des AFT-Pipeline-Workflows erforderlich sind
- AWS CloudTrail (Optional) — Wenn diese Funktion aktiviert ist, erstellt AFT einen AWS CloudTrail Organisationspfad im AWS Control Tower-Verwaltungskonto, um Datenereignisse für Amazon S3-Buckets und AWS Lambda-Funktionen zu protokollieren. AFT sendet diese Protokolle an einen zentralen S3-Bucket im AWS Control Tower-Protokollarchivkonto.
- AWS Support (optional) — Wenn diese Funktion aktiviert ist, aktiviert AFT den AWS Enterprise Support-Plan für von AFT bereitgestellte Konten. Standardmäßig werden AWS Konten mit aktiviertem AWS Basic Support-Plan erstellt.

Pipeline für die Bereitstellung von AFT-Konten

Nachdem die Phase der Kontobereitstellung der Pipeline abgeschlossen ist, wird das AFT-Framework fortgesetzt. Es führt automatisch eine Reihe von Schritten durch, um sicherzustellen, dass die neu bereitgestellten Konten über die entsprechenden Details verfügen, bevor die Anpassungen des Kontos Phase beginnt.

Hier sind die nächsten Schritte, die die AFT-Pipeline ausführt.

1. Validiert die Eingabe der Kontoanforderung.
2. Ruft Informationen über das bereitgestellte Konto ab, z. B. die Konto-ID.

3. Speichert die Kontometadaten in einer DynamoDB-Tabelle im AFT-Verwaltungskonto.
4. Erstellt die AWSaftExecution IAM-Rolle im neu bereitgestellten Konto. AFT übernimmt diese Rolle, um die Phase der Kontoanpassungen durchzuführen, da diese Rolle Zugriff auf das Account Factory-Portfolio gewährt.
5. Wendet die Konto-Tags an, die Sie als Teil der Eingabeparameter für die Kontoanforderung angegeben haben.
6. Wendet die AFT-Funktionsoptionen an, die Sie bei der AFT-Bereitstellung ausgewählt haben.
7. Wendet die von Ihnen bereitgestellten Anpassungen für die AFT-Kontobereitstellung an. Im nächsten Abschnitt erfahren Sie mehr darüber, wie Sie diese Anpassungen mit einer AWS Step Functions-Zustandsmaschine in einem Repository einrichten. `git` Diese Phase wird manchmal als Framework-Phase für die Kontobereitstellung bezeichnet. Sie ist Teil des zentralen Bereitstellungsprozesses, aber Sie haben zuvor ein Framework eingerichtet, das im Rahmen Ihres Workflows zur Kontobereitstellung maßgeschneiderte Integrationen bereitstellt, bevor in der nächsten Phase weitere Anpassungen zu den Konten hinzugefügt werden.
8. Für jedes bereitgestellte Konto wird AWS CodePipeline im AFT-Verwaltungskonto ein Konto erstellt, das ausgeführt wird, um die (nächste, globale) Phase durchzuführen. Anpassungen des Kontos
9. Ruft die Pipeline zur Kontoanpassung für jedes bereitgestellte (und zielgerichtete) Konto auf.
10. Sendet eine Erfolgs- oder Fehlerbenachrichtigung an das SNS-Thema, von dem Sie die Meldungen abrufen können.

Richten Sie die Anpassungen des Frameworks für die Kontobereitstellung mit einer Zustandsmaschine ein

Wenn Sie benutzerdefinierte Integrationen einrichten, die nicht von Terraform stammen, bevor Sie Ihre Konten bereitstellen, sind diese Anpassungen in Ihrem Workflow für die Bereitstellung von AFT-Konten enthalten. Beispielsweise benötigen Sie möglicherweise bestimmte Anpassungen, um sicherzustellen, dass alle von AFT erstellten Konten den Standards und Richtlinien Ihrer Organisation, wie z. B. Sicherheitsstandards, entsprechen. Diese Standards können vor weiteren Anpassungen zu Konten hinzugefügt werden. Diese Anpassungen des Frameworks für die Kontobereitstellung werden auf jedem bereitgestellten Konto implementiert, bevor die nächste Phase der globalen Kontoanpassung beginnt.

> **Note**
>
> Die in diesem Abschnitt beschriebene AFT-Funktion richtet sich an fortgeschrittene Benutzer, die mit der Funktionsweise von AWS Step Functions vertraut sind. Als Alternative empfehlen wir, dass Sie in der Phase der Kontoanpassungen mit den globalen Helfern arbeiten.

Das AFT-Framework für die Kontobereitstellung ruft eine von Ihnen definierte AWS Step Functions-Zustandsmaschine auf, um Ihre Anpassungen zu implementieren. Weitere Informationen zu den möglichen State-Machine-Integrationen finden Sie in der Dokumentation zu AWS Step Functions.

Hier sind einige gängige Integrationen.

- AWS Lambda funktioniert in der Sprache Ihrer Wahl
- AWS ECS- oder AWS Fargate-Aufgaben mithilfe von Docker-Containern
- AWS Step Functions-Aktivitäten mit benutzerdefinierten Mitarbeitern, die entweder in AWS oder vor Ort gehostet werden
- Amazon SNS- oder SQS-Integrationen

Wenn keine AWS Step Functions-Zustandsmaschine definiert ist, wird die Phase mit einem No-Op abgeschlossen. Folgen Sie den Anweisungen unter, um eine Zustandsmaschine für die Bereitstellung von Anpassungen für AFT-Konten zu erstellen. Erstellen Sie Ihre Zustandsmaschine für Anpassungen bei der Bereitstellung Ihres AFT-Kontos Bevor Sie Anpassungen hinzufügen, stellen Sie sicher, dass die Voraussetzungen erfüllt sind.

Diese Arten von Integrationen sind nicht Teil von AWS Control Tower und können während der globalen Pre-API-Phase der AFT-Kontoanpassung nicht hinzugefügt werden. Stattdessen ermöglicht Ihnen die AFT-Pipeline, diese Anpassungen als Teil des Bereitstellungsprozesses einzurichten, und sie werden im Bereitstellungsworkflow ausgeführt. Sie müssen diese Anpassungen implementieren, indem Sie Ihren State Machine im Voraus erstellen, bevor Sie mit der Bereitstellung des AFT-Kontos beginnen, wie in den folgenden Abschnitten beschrieben.

Voraussetzungen für die Erstellung einer Zustandsmaschine

- Ein vollständig eingesetztes AFT. Weitere Informationen Stellen Sie AWS Control Tower Account Factory für Terraform (AFT) bereit zum Einsatz von AFT finden Sie unter.
- Richten Sie in Ihrer Umgebung ein `git` Repository für Anpassungen bei der Bereitstellung von AFT-Konten ein. Weitere Informationen finden Sie unter Post-deployment Schritte.

Erstellen Sie Ihre Zustandsmaschine für Anpassungen bei der Bereitstellung Ihres AFT-Kontos

Schritt 1: Ändern Sie die State-Machine-Definition

Ändern Sie das Beispiel für eine `customizations.asl.json` State-Machine-Definition. Das Beispiel ist in dem `git` Repository verfügbar, das Sie für die Speicherung der Anpassungen der AFT-Kontobereitstellung eingerichtet haben, und zwar in den Schritten nach der Bereitstellung. Weitere Informationen zu State-Machine-Definitionen finden Sie im AWS Step Functions Developer Guide.

Schritt 2: Fügen Sie die entsprechende Terraform-Konfiguration hinzu

Fügen Sie Terraform-Dateien mit der `.tf` Erweiterung in dasselbe `git` Repository mit der State-Machine-Definition für Ihre benutzerdefinierte Integration ein. Wenn Sie sich beispielsweise dafür entscheiden, eine Lambda-Funktion in Ihrer State-Machine-Aufgabendefinition aufzurufen, würden Sie die `lambda.tf` Datei in dasselbe Verzeichnis aufnehmen. Stellen Sie sicher, dass Sie die erforderlichen IAM-Rollen und -Berechtigungen für Ihre benutzerdefinierten Konfigurationen angeben.

Wenn Sie die entsprechenden Eingaben machen, ruft die AFT-Pipeline automatisch Ihren State Machine auf und stellt Ihre Anpassungen als Teil der AFT-Account-Provisioning-Framework-Phase bereit.

Um das Framework für die Bereitstellung von AFT-Konten und die Anpassungen neu zu starten

AFT führt das Framework für die Kontobereitstellung und die Anpassungsschritte für jedes Konto aus, das über die AFT-Pipeline verkauft wird. Um die Anpassungen der Kontobereitstellung erneut zu starten, können Sie eine der beiden folgenden Methoden verwenden:

1. Nehmen Sie im Kontoanforderungs-Repo alle Änderungen an einem vorhandenen Konto vor.
2. Richten Sie ein neues Konto bei AFT ein.

Anpassungen des Kontos

AFT kann Standard- oder benutzerdefinierte Konfigurationen in bereitgestellten Konten bereitstellen. Im AFT-Verwaltungskonto stellt AFT eine Pipeline für jedes Konto bereit. Mit dieser Pipeline können Sie Ihre Anpassungen in allen Konten, in einer Gruppe von Konten oder in einzelnen Konten implementieren. Sie können Python-Skripte, Bash-Skripte und Terraform-Konfigurationen ausführen oder im Rahmen Ihrer Kontoanpassungen mit der AWS-CLI interagieren.

-Übersicht

Nachdem Ihre Anpassungen in den von Ihnen ausgewählten `git` Repositorys angegeben wurden, entweder in dem, in dem Sie Ihre globalen Anpassungen speichern, oder in dem, in dem Sie Ihre Kontoanpassungen speichern, wird die Phase der Kontoanpassungen automatisch von der AFT-Pipeline abgeschlossen. Informationen zur rückwirkenden Anpassung von Konten finden Sie unter. Re-invoke Anpassungen

Globale Anpassungen (optional)

Sie können sich dafür entscheiden, bestimmte Anpassungen auf alle Konten anzuwenden, die von AFT bereitgestellt werden. Wenn Sie beispielsweise eine bestimmte IAM-Rolle erstellen oder in jedem Konto ein benutzerdefiniertes Steuerelement bereitstellen müssen, können Sie dies in der Phase der globalen Anpassungen in der AFT-Pipeline automatisch tun.

Kontoanpassungen (optional)

Um ein einzelnes Konto oder eine Gruppe von Konten anders als andere von AFT bereitgestellte Konten anzupassen, können Sie den Bereich Kontoanpassungen der AFT-Pipeline nutzen, um kontospezifische Konfigurationen zu implementieren. Beispielsweise benötigt möglicherweise nur ein bestimmtes Konto Zugriff auf ein Internet-Gateway.

Voraussetzungen für die Anpassung

Bevor Sie mit der Anpassung von Konten beginnen, stellen Sie sicher, dass diese Voraussetzungen erfüllt sind.

- Ein vollständig bereitgestelltes AFT. Informationen zur Bereitstellung finden Sie unterKonfigurieren und starten Sie Ihre AWS Control Tower Account Factory für Terraform.
- Pre-populated `git`Repositorys für globale Anpassungen und Kontoanpassungen in Ihrer Umgebung. Weitere Informationen finden Sie unter Jedes Repository auffüllen. Post-deployment Schritte

Wenden Sie globale Anpassungen an

Um globale Anpassungen anzuwenden, müssen Sie eine bestimmte Ordnerstruktur in das von Ihnen gewählte Repository übertragen.

- Wenn Ihre benutzerdefinierten Konfigurationen in Form von Python-Programmen oder -Skripten vorliegen, platzieren Sie diese im api_helpers/pythonOrdner Ihres Repositorys.

- Wenn Ihre benutzerdefinierten Konfigurationen in Form von Bash-Skripten vorliegen, platzieren Sie diese im Ordner api_helpers in Ihrem Repository.
- Wenn Ihre benutzerdefinierten Konfigurationen in Form von Terraform vorliegen, platzieren Sie diese im Terraform-Ordner in Ihrem Repository.
- Weitere Informationen zum Erstellen benutzerdefinierter Konfigurationen finden Sie in der README-Datei für globale Anpassungen.

> **Note**
>
> Globale Anpassungen werden automatisch nach der Framework-Phase für die AFT-Kontobereitstellung in der AFT-Pipeline angewendet.

Wenden Sie Kontoanpassungen an

Sie können Kontoanpassungen vornehmen, indem Sie eine bestimmte Ordnerstruktur in das von Ihnen gewählte Repository übertragen. Kontoanpassungen werden automatisch in der AFT-Pipeline und nach der Phase der globalen Anpassungen angewendet. Sie können in Ihrem Repository für Kontoanpassungen auch mehrere Ordner erstellen, die unterschiedliche Kontoanpassungen enthalten. Gehen Sie für jede Kontoanpassung, die Sie benötigen, wie folgt vor.

Um Kontoanpassungen anzuwenden

1. Schritt 1: Erstellen Sie einen Ordner für eine Kontoanpassung

   Kopieren Sie in Ihrem ausgewählten Repository den von AFT bereitgestellten `ACCOUNT_TEMPLATE` Ordner in einen neuen Ordner. Der Name Ihres neuen Ordners sollte mit dem Namen übereinstimmen`account_customizations_name`, den Sie in Ihrer Kontoanfrage angegeben haben.
2. Fügen Sie die Konfigurationen Ihrem spezifischen Kontoanpassungsordner hinzu

   Sie können Ihrem Ordner mit Kontoanpassungen Konfigurationen hinzufügen, die auf dem Format Ihrer Konfigurationen basieren.

   - Wenn Ihre benutzerdefinierten Konfigurationen in Form von Python-Programmen oder -Skripten vorliegen, platzieren Sie sie im api_helpers/python Ordner ***`[account_customizations_name]`***/in Ihrem Repository.

- Wenn Ihre benutzerdefinierten Konfigurationen in Form von Bash-Skripten vorliegen, platzieren Sie sie im Ordner ***[account_customizations_name]***/api_helpers in Ihrem Repository.
- Wenn Ihre benutzerdefinierten Konfigurationen in Form von Terraform vorliegen, platzieren Sie sie im Ordner ***[account_customizations_name]***/terraform, der sich in Ihrem Repository befindet.

Weitere Informationen zum Erstellen benutzerdefinierter Konfigurationen finden Sie in der README-Datei für Kontoanpassungen.

3. Beziehen Sie sich auf den spezifischen **`account_customizations_name`** Parameter in der Kontoanforderungsdatei

   Die AFT-Kontoanforderungsdatei enthält den Eingabeparameter`account_customizations_name`. Geben Sie den Namen Ihrer Kontoanpassung als Wert für diesen Parameter ein.

> **Note**
>
> Sie können mehrere Kontoanfragen für Konten in Ihrer Umgebung einreichen. Wenn Sie unterschiedliche oder ähnliche Kontoanpassungen anwenden möchten, geben Sie die Kontoanpassungen mithilfe des `account_customizations_name` Eingabeparameters in Ihren Kontoanfragen an. Weitere Informationen finden Sie unter Mehrere Kontoanfragen einreichen.

Re-invoke Anpassungen

AFT bietet eine Möglichkeit, Anpassungen in der AFT-Pipeline erneut aufzurufen. Diese Methode ist nützlich, wenn Sie einen neuen Anpassungsschritt hinzugefügt haben oder wenn Sie Änderungen an einer vorhandenen Anpassung vornehmen. Wenn Sie erneut aufrufen, initiiert AFT die Anpassungspipeline, um Änderungen am bereitgestellten AFT-Konto vorzunehmen. Ein erneuter Aufruf auf der Grundlage einer Ereignisquelle ermöglicht es Ihnen, Anpassungen auf einzelne Konten, auf alle Konten, auf Konten gemäß ihrer Organisationseinheit oder auf Konten, die anhand von Stichwörtern ausgewählt wurden, anzuwenden.

Folgen Sie diesen drei Schritten, um Anpassungen für Konten erneut aufzurufen. AFT-provisioned

Schritt 1: Änderungen an globale Repositorys oder Repositorys für Kontoanpassungen weiterleiten **`git`**

Sie können Ihre globalen Anpassungen und Kontoanpassungen nach Bedarf aktualisieren und Änderungen zurück in Ihre Repositorys übertragen. `git` Zu diesem Zeitpunkt passiert nichts. Die Anpassungspipeline muss von einer Ereignisquelle aufgerufen werden, wie in den nächsten beiden Schritten erklärt.

Schritt 2: Starten Sie eine AWS Step Function-Ausführung, um Anpassungen erneut aufzurufen

AFT bietet eine AWS-Step-Funktion, die `aft-invoke-customizations` im AFT-Verwaltungskonto aufgerufen wird. Der Zweck dieser Funktion besteht darin, die Anpassungspipeline für AFT-provisioned Konten erneut aufzurufen.

Hier ist ein Beispiel für ein Ereignisschema (JSON-Format), das Sie erstellen können, um Eingaben an die `aft-invoke-customizations` AWS Step Function zu übergeben.

```
{
  "include": [
    {
      "type": "all"
    },
    {
      "type": "ous",
      "target_value": [ "ou1","ou2"]
    },
    {
      "type": "tags",
      "target_value": [ {"key1": "value1"}, {"key2": "value2"}]
    },
    {
      "type": "accounts",
      "target_value": [ "acc1_ID","acc2_ID"]
    }
  ],

  "exclude": [
    {
      "type": "ous",
      "target_value": [ "ou1","ou2"]
    },
    {
```

```
      "type": "tags",
      "target_value": [ {"key1": "value1"}, {"key2": "value2"}]
    },
    {
      "type": "accounts",
      "target_value": [ "acc1_ID","acc2_ID"]
    }
  ]
}
```

Das Beispiel-Eventschema zeigt, dass Sie Konten auswählen können, die in den erneuten Aufrufprozess aufgenommen oder davon ausgeschlossen werden sollen. Sie können nach Organisationseinheit (OU), Konto-Tags und Konto-ID filtern. Wenn Sie keine Filter anwenden und den Kontoauszug hinzufügen`"type":"all"`, wird die Anpassung für alle AFT-provisioned Konten erneut aufgerufen.

Sie können einen `bypass_steps` Parameter in die Step Functions Functions-Eingabe aufnehmen, um bestimmte Bereitstellungsphasen während des erneuten Aufrufs zu überspringen.

`bypass_steps` Wert	Behavior
`["provisioning_bootstrap"]`	Überspringt die Phasen Kontobereitstellung und Bootstrap; führt nur Konto- und globale Anpassungspipelines aus.
`[]`(leer)	Führt den gesamten Ablauf einschließlich der Bereitstellung aus (Standard).

Das folgende Beispiel zeigt eine Step Functions Functions-Eingabe, die Anpassungen für ein bestimmtes Konto erneut aufruft und dabei Bereitstellungs- und Bootstrap-Schritte umgeht.

```
{
  "include": [
    {
      "type": "accounts",
      "target_value": ["123456789012"]
    }
  ],
  "bypass_steps": ["provisioning_bootstrap"]
}
```

> **Note**
>
> Wenn Ihre Version von AWS Control Tower Account Factory for Terraform (AFT) 1.6.5 oder höher ist, können Sie verschachtelte OUs mit der Syntax als Ziel verwenden). `OU Name (ou-id-1234` Weitere Informationen finden Sie im folgenden Thema unter. GitHub

Wenn Sie eine Vorschau der Änderungen anzeigen möchten, die AFT an einem Konto vornehmen würde, ohne sie zu übernehmen, verwenden Sie einen Testlauf, der nur für den Tarif gilt. Um einen zu starten, fügen Sie `true` in die Step Functions Functions-Eingabe einen `plan_only` Parameter ein, der auf gesetzt ist. Wenn Sie diese Einstellung vornehmen`"plan_only": true`, wird AFT stattdessen `terraform plan` für Ihre globalen Anpassungen und Kontoanpassungen ausgeführt. `terraform apply` Sie können dann überprüfen, welche Änderungen ein Konto erhalten würde, bevor Sie sie anwenden. Plan-only läuft auf allen unterstützten Terraform-Distributionen, einschließlich Community Edition, HCP Terraform (Terraform Cloud) und Terraform Enterprise.

Das folgende Beispiel zeigt eine Step Functions Functions-Eingabe, die einen reinen Planlauf für ein bestimmtes Konto durchführt, indem `plan_only` die Konto-ID im `include` Block festgelegt `true` und angegeben wird.

```
{
  "include": [
    {
      "type": "accounts",
      "target_value": ["123456789012"]
    }
  ],
  "plan_only": true
}
```

Ersetzen Sie im vorherigen Beispiel den folgenden Wert durch Ihre eigenen Informationen:

- `123456789012`— Ersetzen Sie diesen Wert durch die AWS-Konto-ID, die Sie für den reinen Planlauf als Ziel verwenden möchten.

Nachdem Sie die Planausgabe überprüft haben, führen Sie die Anpassungspipeline ohne den `plan_only` Parameter erneut aus (eine normale Ausführung), um die Änderungen auf Ihre Konten anzuwenden.

> **Note**
>
> Bei der Community Edition-Distribution (Open Source) exportiert AFT die JSON-Ausgabe jedes Plans in den verschlüsselten Amazon S3 S3-Bucket mit Planausgabe im AFT-Verwaltungskonto. Dieser Export erfolgt bei jeder Ausführung, bei der nur ein Plan verfügbar ist. In den Distributionen HCP Terraform (Terraform Cloud) und Terraform Enterprise können Sie die Planergebnisse in der HCP Terraform Run-Benutzeroberfläche anzeigen. Sie können optional auch die JSON-Ausgabe jedes Plans in den Bucket exportieren. Weitere Informationen finden Sie unter Exportieren Sie die Terraform-Planausgabe nach Amazon S3.

Nachdem Sie die Ereignisparameter ausgefüllt haben, wird Step Functions ausgeführt und ruft die entsprechenden Anpassungen auf. AFT kann maximal 5 Anpassungen gleichzeitig aufrufen. Step Functions wartet und wiederholt, bis alle Konten, die den Ereigniskriterien entsprechen, vollständig sind.

Schritt 3: Überwachen Sie die AWS Step Function-Ausgabe und beobachten Sie, wie AWS CodePipeline läuft

- Die resultierende Step Function-Ausgabe enthält Konto-IDs, die mit der Step Function-Eingabeereignisquelle übereinstimmen.
- Navigieren Sie CodePipeline unter Developer Tools zu AWS und sehen Sie sich die entsprechenden Anpassungspipelines für die Konto-ID an.

Fehlerbehebung bei der Rückverfolgung von Anfragen zur AFT-Kontoanpassung

Workflows zur Kontoanpassung, die auf Emissionsprotokollen AWS Lambda basieren, die IDs für Zielkonten und Anpassungsanfragen enthalten. AFT ermöglicht es Ihnen, Anpassungsanfragen mit Amazon CloudWatch Logs zu verfolgen und zu beheben, indem es Ihnen CloudWatch Logs Insights-Abfragen zur Verfügung stellt, mit denen Sie CloudWatch Logs zu Ihrer Anpassungsanfrage nach Ihrem Zielkonto oder Ihrer Personalisierungsanforderungs-ID filtern können. Weitere Informationen finden Sie unter Analysieren von Protokolldaten mit Amazon CloudWatch Logs im Amazon CloudWatch Logs-Benutzerhandbuch.

Um CloudWatch Logs Insights für AFT zu verwenden

1. Öffnen Sie die CloudWatch Konsole unter https://console.aws.amazon.com/cloudwatch/.
2. Wählen Sie im Navigationsbereich Logs und dann Logs Insights aus.

3. Wählen Sie Abfragen aus.
4. Wählen Sie unter Beispielabfragen die Option Account Factory for Terraform und wählen Sie dann eine der folgenden Abfragen aus:

   - Anpassungsprotokolle nach Konto-ID

   > **Note**
   >
   > Stellen Sie sicher, dass Sie es *"YOUR-ACCOUNT-ID"* durch Ihre Zielkonto-ID ersetzen.

   ```
   fields @timestamp, log_message.account_id as target_account_id,
    log_message.customization_request_id as customization_request_id,
    log_message.detail as detail, @logStream
   | sort @timestamp desc
   | filter log_message.account_id == "YOUR-ACCOUNT-ID" and @message like /
   customization_request_id/
   ```

   - Anpassungsprotokolle nach der ID der Anpassungsanforderung

   > **Note**
   >
   > Stellen Sie sicher, dass Sie es *"YOUR-CUSTOMIZATION-REQUEST-ID"* durch Ihre Personalisierungsanforderungs-ID ersetzen. Sie finden Ihre Anpassungsanforderungs-ID in der Ausgabe der AWS Step Functions State-Machine des AFT-Account-Provisioning-Frameworks. Weitere Informationen zum Framework für die AFT-Kontobereitstellung finden Sie unter Pipeline zur AFT-Kontobereitstellung

   ```
   fields @timestamp, log_message.account_id as target_account_id,
    log_message.customization_request_id as customization_request_id,
    log_message.detail as detail, @logStream
   | sort @timestamp desc
   | filter log_message.customization_request_id == "YOUR-CUSTOMIZATION-REQUEST-ID"
   ```

5. Nachdem Sie eine Abfrage ausgewählt haben, stellen Sie sicher, dass Sie ein Zeitintervall auswählen, und wählen Sie dann Abfrage ausführen aus.

Auslöser für die Anpassung

Die Anpassungsauslöser von Account Factory for Terraform (AFT) automatisieren die erneute Ausführung von Konto- und globalen Anpassungen, wenn Konten zwischen Organisationseinheiten (OUs) verschoben werden. Im Zuge der Weiterentwicklung Ihrer Organisation wechseln Konten häufig zwischen Organisationseinheiten, um Änderungen in Bezug auf Teamverantwortung, Compliance-Anforderungen oder Workload-Klassifizierung widerzuspiegeln. Ohne Anpassungsauslöser erfordert jeder Schritt ein manuelles Eingreifen, um die Anpassungen, die dem neuen Unternehmenskontext des Accounts entsprechen, erneut anzuwenden.

Wenn Anpassungsauslöser aktiviert sind, erkennt AFT Änderungen an der Organisationseinheit und ruft automatisch Ihre Anpassungspipelines für die betroffenen Konten auf. Dadurch wird sichergestellt, dass Konten immer die Anpassungen vornehmen, die ihrer aktuellen Platzierung in der Organisationseinheit entsprechen, wodurch der betriebliche Aufwand reduziert und das Risiko von Konfigurationsabweichungen minimiert wird. Wenn ein Konto beispielsweise von einer Entwicklungs-OU zu einer Produktionsorganisationseinheit wechselt, können mithilfe von Anpassungsauslösern automatisch produktionsspezifische Sicherheitskontrollen und Compliance-Richtlinien angewendet werden, ohne dass manuelles Eingreifen erforderlich ist.

> **Important**
>
> Konten, die über die Auto Enroll-Funktion in der AWS Control Tower Tower-Landing landing zone aktualisiert wurden, geben das `UpdateManagedAccount` Lifecycle-Ereignis nicht aus. Anpassungsauslöser werden bei diesen Vorgängen nicht ausgelöst. Wenn Sie sich auf Auto Enroll verlassen, um Konten unter die Verwaltung von AWS Control Tower zu stellen, müssen Sie die Anpassungen für diese Konten manuell erneut aufrufen.

So funktionieren Anpassungsauslöser

Wenn Anpassungsauslöser aktiviert sind und AFT ein Ereignis zur Kontobereitstellung verarbeitet, bewertet es, ob sich die Organisationseinheit des Kontos geändert hat, und ergreift die entsprechenden Maßnahmen.

1. AFT erkennt eine Änderung der Organisationseinheit, indem es die aktuelle Organisationseinheit des Kontos mit der zuvor erfassten Organisationseinheit vergleicht.
2. Wenn sich die Organisationseinheit geändert hat, bereichert AFT die Ausführung um den Triggerkontext, einschließlich der Quell- und Ziel-OU.

3. AFT ruft die Anpassungspipeline auf und umgeht dabei die Bereitstellungs- und Bootstrap-Schritte, die bereits abgeschlossen wurden. Einzelheiten zur Bypass-Konfiguration finden Sie unter. the section called “Re-invoke Anpassungen”
4. AFT zeichnet einen Auditeintrag mit den Ausgangs- und Zielkonten des Auslösers auf.

Wenn die Funktion deaktiviert ist oder wenn sich die Organisationseinheit nicht geändert hat, wird die Standardbereitstellung fortgesetzt, ohne dass die Anpassung erneut ausgeführt wird.

Konfiguration von Auslösern für Anpassungen

Um Anpassungsauslöser zu aktivieren, legen Sie die `aft_customization_triggers` Variable in Ihrem AFT-Bereitstellungsmodul fest:

```
module "aft" {
  source = "github.com/aws-ia/terraform-aws-control_tower_account_factory"

  aft_customization_triggers = ["account_move"]

  # ... other variables
}
```

Der einzige gültige Wert ist `"account_move"`. Um Anpassungsauslöser zu deaktivieren, setzen Sie die Variable auf eine leere Liste (`[]`). Die Funktion ist standardmäßig deaktiviert.

Um ein bestimmtes Konto von der automatischen Triggerverarbeitung auszuschließen, setzen Sie das `account_skip_customization_triggers` Attribut `"true"` für das Zielkonto in der Terraform-Datei für die Kontoanforderung auf. Wenn dieses Attribut festgelegt ist, überspringt AFT den Aufruf der Anpassung für dieses Konto, selbst wenn es eine Änderung der Organisationseinheit feststellt. Dies ist nützlich für Konten, bei denen geplante Migrationen durchgeführt werden, bei denen eine automatische Anpassung nicht erwünscht ist.

Unterstützte Ereignispfade

Der `account_move` Trigger wird ausgelöst, wenn AFT ein `UpdateManagedAccount` AWS Control Tower Tower-Lifecycle-Ereignis empfängt. Dieses Ereignis wird ausgelöst, wenn:

- Die Organisationseinheit eines Kontos wird über die AFT-Kontoanforderungsdatei (`ManagedOrganizationalUnit`Terraform-Parameter-Update) geändert.
- Ein Konto wird über die AWS Control Tower Tower-Konsole aktualisiert.

- Ein Konto wird mithilfe der Operationen Register OU oder Account Factory (Konsole oder Service Catalog API) verschoben.

> **Important**
>
> Konten, die über die Auto Enroll-Funktion in der AWS Control Tower Tower-Landing landing zone aktualisiert wurden, geben das `UpdateManagedAccount` Lifecycle-Ereignis nicht aus. Der Anpassungsauslöser wird bei diesen Vorgängen nicht ausgelöst.

Weitere Informationen zu den Lebenszyklusereignissen von AWS Control Tower finden Sie unter Lifecycle-Ereignisse im AWS Control Tower Tower-Benutzerhandbuch.

Überwachung und Rückverfolgbarkeit

Bei jeder Anpassungsausführung (unabhängig davon, ob sie durch eine Änderung der Organisationseinheit, einen manuellen Aufruf oder eine Kontoanforderung ausgelöst wird) wird ein Auditdatensatz in eine DynamoDB-Tabelle geschrieben. Anhand dieser Datensätze können Sie nachvollziehen, warum eine Anpassung ausgeführt wurde, welche Konten betroffen waren und wie sich die Ausführung auf andere Pipeline-Aktivitäten bezieht.

Feld	Description
`execution_id`	Die Ausführungs-ID von Step Functions
`timestamp`	Wann der Datensatz erstellt wurde
`target_accounts`	Liste der Zielkonto-IDs
`bypass_steps`	Schritte zur Bereitstellung, die übersprungen wurden
`customization_triggers`	Triggerkontext (Quell- und Ziel-OU)
`trigger_source`	Warum wurde die Ausführung ausgeführt:`account_move` ,`manual`, oder `account_request`
`customization_request_id`	Verbindet die Bereitstellungs- und Anpassungsausführungen für eine durchgängige Korrelation

Auf diese `customization_request_id` Weise können Sie das auslösende Ereignis mit der Downstream-Pipeline-Ausführung über beide Step Functions Functions-Zustandsmaschinen hinweg korrelieren. Sie können diese Kennung verwenden, um die Bewegung eines einzelnen Kontos von der ersten Erkennung bis zum Abschluss der Anpassung nachzuverfolgen.

Example Auditdatensätze nach Triggerquelle abfragen

```
aws dynamodb scan \
  --table-name aft-customizations-audit \
  --filter-expression "trigger_source = :ts" \
  --expression-attribute-values '{":ts": {"S": "account_move"}}'
```

Alternativen zur Versionskontrolle von Quellcode in AFT

AFT AWS CodeCommit verwendet als Quellcode-Versionskontrollsystem (VCS) und ermöglicht andere, AWS CodeConnectionsdie Ihren Geschäftsanforderungen oder der vorhandenen Architektur entsprechen.

Wenn Sie AFT zum ersten Mal bereitstellen und noch kein CodeCommit Repository haben, müssen Sie im Rahmen der AFT-Bereitstellungsvoraussetzungen einen externen VCS-Anbieter angeben.

AFT unterstützt die folgenden Alternativen zur Quellcodeverwaltung:

- GitHub
- GitHub Unternehmensserver
- BitBucket
- GitLab
- GitLab Self-managed
- Azure DevOps

> **Note**
>
> Wenn Sie es AWS CodeCommit als Ihr VCS angeben, sind keine zusätzlichen Schritte erforderlich. AFT erstellt die erforderlichen `git` Repositorys in Ihrer Umgebung mit Standardnamen. Sie können jedoch die Standard-Repository-Namen bei CodeCommit Bedarf überschreiben, um Ihren Unternehmensstandards zu entsprechen.

Richten Sie mit AFT ein alternatives Quellcode-Versionskontrollsystem (benutzerdefiniertes VCS) ein

Gehen Sie folgendermaßen vor, um ein alternatives Quellcode-Versionskontrollsystem für Ihre AFT-Bereitstellung einzurichten.

Schritt 1: Erstellen Sie **`git`** Repositorys in einem unterstützten Versionskontrollsystem (VCS) eines Drittanbieters.

Wenn Sie es nicht verwenden AWS CodeCommit, müssen Sie `git` Repositorys in Ihrer AFT-supported VCS-Anbieterumgebung eines Drittanbieters für die folgenden Elemente erstellen.

- AFT-Kontoanfragen. Beispielcode verfügbar. Weitere Informationen zu AFT-Kontoanfragen finden Sie unterStellen Sie ein neues Konto bei AFT bereit.
- Anpassungen bei der Bereitstellung von AFT-Konten. Beispielcode verfügbar. Weitere Informationen zu Anpassungen der AFT-Kontobereitstellung finden Sie unter. Erstellen Sie Ihre Zustandsmaschine für Anpassungen bei der Bereitstellung Ihres AFT-Kontos
- Globale AFT-Anpassungen. Beispielcode verfügbar. Weitere Informationen zu globalen AFT-Anpassungen finden Sie unterAnpassungen des Kontos.
- Anpassungen des AFT-Kontos. Beispielcode verfügbar. Weitere Informationen zu AFT-Kontoanpassungen finden Sie unterAnpassungen des Kontos.

Schritt 2: Geben Sie die für die AFT-Bereitstellung erforderlichen VCS-Konfigurationsparameter an

Die folgenden Eingabeparameter werden benötigt, um Ihren VCS-Anbieter im Rahmen der AFT-Bereitstellung zu konfigurieren.

- vcs_provider: Wenn Sie nicht verwenden AWS CodeCommit, geben Sie den VCS-Anbieter je nach `"bitbucket"` Anwendungsfall als `"github""githubenterprise","gitlab",, "gitlabselfmanaged""azuredevops"`, oder an.
- github_enterprise_url: Geben Sie die URL nur für Unternehmenskunden an. GitHub GitHub
- account_request_repo_name: Für Benutzer ist dieser Wert auf gesetzt. AWS CodeCommit `aft-account-request` Aktualisieren Sie diesen AFT-supported Eingabewert in einer VCS-Anbieterumgebung eines Drittanbieters mit Ihrem tatsächlichen Repository-Namen. Für Github BitBucket, GitHub Enterprise, GitLab GitLab Self-managed, und Azure DevOps muss der Repository-Name das Format `[Org]/[Repo]` haben.

- account_customizations_repo_name: Für Benutzer ist dieser Wert auf gesetzt. AWS CodeCommit `aft-account-customizations` Aktualisieren Sie diesen Eingabewert in einer AFT-supported VCS-Anbieterumgebung eines Drittanbieters mit Ihrem Repository-Namen. Für Github BitBucket, GitHub Enterprise, GitLab GitLab Self-managed, und Azure DevOps muss der Repository-Name das Format `[Org]/[Repo]` haben.
- account_provisioning_customizations_repo_name: Für Benutzer ist dieser Wert auf gesetzt. AWS CodeCommit `aft-account-provisioning-customizations` Aktualisieren Sie diesen Eingabewert in einer Umgebung eines VCS-Anbieters eines Drittanbieters AFT-supported mit Ihrem Repository-Namen. Für Github BitBucket, GitHub Enterprise, GitLab GitLab Self-managed, und Azure DevOps muss der Repository-Name das Format `[Org]/[Repo]` haben.
- global_customizations_repo_name: Für Benutzer ist dieser Wert auf gesetzt. AWS CodeCommit `aft-global-customizations` Aktualisieren Sie diesen Eingabewert in einer AFT-supported VCS-Anbieterumgebung eines Drittanbieters mit Ihrem Repository-Namen. Für Github BitBucket, GitHub Enterprise, GitLab GitLab Self-managed, und Azure DevOps muss der Repository-Name das Format `[Org]/[Repo]` haben.
- account_request_repo_branch: Der Branch ist `main` standardmäßig, aber der Wert kann überschrieben werden.

Standardmäßig stammen AFT-Quellen aus dem Branch jedes Repositorys. `main` `git` Sie können den Wert des Zweignamens mit einem zusätzlichen Eingabeparameter überschreiben. Weitere Informationen zu Eingabeparametern finden Sie in der README-Datei im AFT-Terraform-Modul.

> **Für bestehende AWS CodeCommit Kunden**
>
> Wenn Sie ein CodeCommit Repository mit einem neuen Namen für AFT erstellen, können Sie den Repository-Namen aktualisieren, indem Sie die Werte für diese Eingabeparameter aktualisieren.

Schritt 3: Stellen Sie die AWS CodeCommit Verbindung für VCS-Drittanbieter her

Wenn Ihre Bereitstellung ausgeführt wird, erstellt AFT entweder die erforderlichen AWS CodeCommit Repositorys oder eine AWS CodeCommit Verbindung für den von Ihnen ausgewählten VCS-Drittanbieter. Im letzteren Fall müssen Sie sich manuell bei der Konsole des AFT-Verwaltungskontos anmelden, um die ausstehende CodeCommit Verbindung herzustellen. Weitere Anweisungen zum AWS CodeCommit Herstellen der CodeCommit Verbindung finden Sie in der Dokumentation.

Verschiebe AFT von AWS CodeCommit zu einem anderen VCS-Anbieter

Dieser Abschnitt bietet einen Überblick darüber, wie Sie AWS Control Tower Account Factory for Terraform (AFT) von AWS CodeCommit Ihrem Versionskontrollsystem (VCS) zu einem anderen VCS-Anbieter migrieren können.

Schritt 1. Richten Sie neue Repositorys im VCS Ihrer Wahl ein.

Schritt 2. Fügen Sie diese Repositorys als neue Remotes hinzu. `git`

Schritt 3. Führen Sie die Ausführung `git push` zum neuen VCS-Anbieter aus.

> **Note**
>
> Die Repository-Struktur, die Sie erstellen, sollte dieselbe sein wie in AWS CodeCommit. Eine Änderung der Struktur beeinträchtigt die Fähigkeit von AFT, den gewünschten Code auszuführen.
>
> Struktur des Repositorys:
>
> - nach einer Kontoanfrage
> - aft-Account-Anpassungen
> - aft-global-anpassungen
> - aft-account-provisioning-anpassungen

Schritt 4. Aktualisieren Sie in Ihrem AWS Control Tower-Verwaltungskonto das Terraform-Modul (Bootstrap) so, dass es auf Ihren VCS-Anbieter verweist, wie im folgenden Beispiel gezeigt:

Beispiel: mit Terraform OSS GitLab

— Führen Sie dann aus`terraform plan`, um eine Vorschau der Änderungen anzuzeigen. `terraform apply`

Schritt 5. Gehen Sie wie folgt vor, um die Einrichtung von CodeConnection (früher bekannt als CodeStar) abzuschließen:

1. Melden Sie sich bei Ihrem AFT-Verwaltungskonto an
2. Suchen Sie nach dem Ausstehenden AWS CodeConnections für den neuen VCS-Anbieter und schließen Sie ihn ab, wie unter Eine ausstehende Verbindung https://docs.aws.amazon.com/

dtconsole/latest/userguide/connections-update.html aktualisieren oder in der AWS Konsole [`https://us-east-1.console.aws.amazon.com/codesuite/settings/connections`] beschrieben.

3. Referenz: Schritte Post-deployment

> **Note**
>
> Account-Pipelines behalten die vorherige Quelle bei, bis `aft-invoke-customizations` Step Functions aufgerufen wird. Dieser Aufruf kann als Teil des Upgrades oder als Teil der nächsten Anpassungsaufrufe erfolgen.

Weitere Informationen findest du in diesem Blog: So migrierst du dein AWS CodeCommit Repository zu einem anderen Git-Anbieter.

Datenschutz

Das Modell der AWS gemeinsamen Verantwortung gilt für den Datenschutz bei AFT. Aus Datenschutzgründen empfehlen wir die folgenden bewährten Sicherheitsmethoden.

- Folgen Sie den Datenschutzrichtlinien von AWS Control Tower. Details hierzu finden Sie unter Datenschutz in AWS Control Tower.
- Behalten Sie die Terraform-Status-Konfiguration bei, die zum Zeitpunkt der AFT-Bereitstellung generiert wurde. Details hierzu finden Sie unter Stellen Sie AWS Control Tower Account Factory für Terraform (AFT) bereit.
- Wechseln Sie vertrauliche Anmeldeinformationen regelmäßig, wie es die Sicherheitsrichtlinien Ihres Unternehmens vorsehen. Beispiele für Geheimnisse sind `git` Terraform-Token, Tokens usw.

Verschlüsselung im Ruhezustand

AFT erstellt Amazon S3-Buckets, Amazon SNS-Themen, Amazon SQS-Warteschlangen und Amazon DynamoDB-Datenbanken, die im Ruhezustand mit Key Management Service-Schlüsseln verschlüsselt werden. AWS Bei KMS-Schlüsseln, die von AFT erstellt wurden, ist die jährliche Rotation standardmäßig aktiviert. Wenn Sie die HCP Terraform- oder Terraform Enterprise-Distributionen von Terraform wählen, enthält AFT einen AWS Systems SecureString Manager-Parameter zum Speichern sensibler Terraform-Tokenwerte.

AFT verwendet die hier beschriebenen AWS Dienste, die im Komponentendienste Ruhezustand standardmäßig verschlüsselt werden. Einzelheiten finden Sie in der AWS Dokumentation zu den einzelnen AWS Diensten von AFT. Informieren Sie sich auch über die Datenschutzpraktiken der einzelnen Dienste.

Verschlüsselung während der Übertragung

AFT stützt sich auf Komponentendienste die unter beschriebenen AWS Dienste, die standardmäßig Verschlüsselung bei der Übertragung verwenden. Einzelheiten finden Sie in der AWS Dokumentation zu den einzelnen AWS Diensten von AFT. Informieren Sie sich auch über die Datenschutzpraktiken der einzelnen Dienste.

Bei HCP Terraform- oder Terraform Enterprise-Distributionen ruft AFT eine HTTPS-Endpunkt-API für den Zugriff auf Ihre Terraform-Organisation auf. Wenn Sie einen VCS-Drittanbieter wählen, der von AWS CodeStar Verbindungen unterstützt wird, ruft AFT eine HTTPS-Endpunkt-API für den Zugriff auf Ihre VCS-Anbieterorganisation auf.

Ein Konto aus AFT entfernen

In diesem Thema wird beschrieben, wie ein Konto aus AFT entfernt wird, sodass die AFT-Pipeline die Bereitstellung und Aktualisierung des Kontos beendet.

> **Important**
>
> Das Entfernen eines Kontos aus der AFT-Pipeline ist irreversibel und kann zu einem Statusverlust führen.

Sie können ein Konto aus AFT entfernen, wenn Sie ein Konto für eine stillgelegte Anwendung schließen, ein kompromittiertes Konto isolieren oder ein Konto von einer Organisation in eine andere verschieben möchten.

> **Note**
>
> Das Entfernen eines Kontos aus AFT unterscheidet sich vom Löschen eines AWS Control Tower Tower-Kontos oder AWS-Konto. Wenn Sie ein Konto aus AFT entfernen, verwaltet AWS Control Tower das Konto weiterhin. Um ein AWS Control Tower Tower-Konto zu löschen AWS-Konto, oder gehen Sie wie folgt vor:
>
> - Im AWS Control Tower Tower-Benutzerhandbuch die Verwaltung eines Kontos aufheben.

- Ein Konto schließen im AWS Billing Benutzerhandbuch.

Um ein Konto aus den AFT-Pipelines zu entfernen

Das folgende Verfahren beschreibt, wie Sie ein Konto aus AFT entfernen.

1. Entfernen Sie das Konto aus dem **`git`** Repository, in dem Kontoanfragen gespeichert sind

   Löschen Sie in dem `git` Repository, in dem Sie Kontoanfragen speichern, die Kontoanfrage für das Konto, das Sie aus AFT entfernen möchten.

   Wenn Sie eine Kontoanfrage aus dem Kontoanforderungs-Repository entfernen, löscht AFT die Anpassungspipeline und die Konto-Metadaten. Weitere Informationen finden Sie in den Versionshinweisen für AFT 1.8.0 unter. GitHub
2. Terraform Workspace löschen (nur für HCP Terraform- und Terraform Enterprise-Kunden)

   Löschen Sie die Arbeitsbereiche für globale Anpassungen und Kontoanpassungen für das Konto, das Sie aus AFT entfernen möchten.
3. Terraform-Status aus dem Amazon S3 S3-Backend löschen

   Löschen Sie im AFT-Verwaltungskonto alle relevanten Ordner in den Amazon S3 S3-Buckets für das Konto, das Sie aus AFT entfernen möchten.

   > **Tip**
   >
   > Ersetzen Sie es in den folgenden Beispielen *`012345678901`* durch die ID-Nummer des AFT-Verwaltungskontos.

   Beispiel: Terraform OSS

   Wenn Sie sich für Terraform OSS entscheiden, finden Sie 3 Ordner für jedes Konto in den Buckets `aft-backend-`*`012345678901`*`-primary-region` und `aft-backend-`*`012345678901`*`-secondary-region` Amazon S3. Diese Ordner beziehen sich auf den Status der Kontoanpassungen, den Status der Anpassungspipeline und den Status der globalen Anpassungen

   Beispiel: HCP Terraform oder Terraform Enterprise

Wenn Sie sich für HCP Terraform oder Terraform Enterprise entscheiden, finden Sie einen Ordner für jedes Konto in den `aft-backend-012345678901-primary-region` Buckets und Amazon S3. `aft-backend-012345678901-secondary-region` Diese Ordner beziehen sich auf den Status der Anpassungs-Pipeline.

Operationelle Metriken

Standardmäßig sendet Account Factory for Terraform (AFT) anonyme Betriebsmetriken an. AWS Wir verwenden diese Daten, um zu verstehen, wie Kunden AFT verwenden, sodass wir die Qualität und die Funktionen der Lösung verbessern können. Sie können die Datenerfassung deaktivieren, indem Sie während der AFT-Bereitstellung einen Parameter ändern. Wenn die Erfassung aktiviert ist, werden die folgenden Daten gesendet an AWS:

- Lösung: Die AFT-spezifische Kennung
- Version: Die Version von AFT
- Universally Unique Identifier (UUID): Zufällig generierter, eindeutiger Bezeichner für jede AFT-Bereitstellung
- Zeitstempel: Zeitstempel der Datenerfassung
- Daten: AFT-Konfiguration und vom Kunden ergriffene Maßnahmen

AWS besitzt die gesammelten Daten. Die Datenerfassung unterliegt der AWS Datenschutzrichtlinie.

> **Note**
>
> Versionen von AFT vor 1.6.0 melden keine Nutzungsmetriken an AWS.

So deaktivieren Sie die Berichterstattung über Metriken:

- Stellen Sie `false` in Ihrer Terraform-Eingabekonfigurationsdatei den Eingabewert auf ein, wie im folgenden Beispiel gezeigt, und stellen Sie AFT erneut bereit. `aft_metrics_reporting` Dieser Wert ist `true` standardmäßig auf festgelegt, wenn Sie ihn nicht explizit festlegen.

Wenn Sie das Beispiel kopieren, denken Sie daran, die in Zeichenketten angegebenen Elemente durch Ihre tatsächlichen ID- und Regionswerte durch zu ersetzen`x`.

```
module "control_tower_account_factory" {
source = "aws-ia/control_tower_account_factory/aws"

# Required Vars
ct_management_account_id    = "xxxxxxxxxxx"
log_archive_account_id      = "xxxxxxxxxxx"
audit_account_id            = "xxxxxxxxxxx"
aft_management_account_id   = "xxxxxxxxxxx"
ct_home_region              = "xx-xxxx-x"
tf_backend_secondary_region = "xx-xxxx-x"

# Optional Vars
aft_metrics_reporting = false    # to opt out, set this value to false
}
```

Leitfaden zur Fehlerbehebung bei Account Factory for Terraform (AFT)

Dieser Abschnitt kann Ihnen bei der Behebung häufig auftretender Probleme helfen, die bei der Verwendung von Account Factory for Terraform (AFT) auftreten können.

Themen

- Allgemeine Probleme
- Probleme im Zusammenhang mit dem Konto provisioning/registration
- Probleme im Zusammenhang mit dem Aufrufen von Anpassungen
- Probleme im Zusammenhang mit dem Workflow zur Kontoanpassung

Allgemeine Probleme

- Ressourcenkontingente überschritten AWS

  Wenn Ihre Protokollgruppen darauf hinweisen, dass Sie die AWS Ressourcenkontingente überschritten haben, wenden Sie sich an den AWS Support. Account Factory verwendet AWS-Services mit Ressourcenkontingenten, die AWS CodeBuild AWS Organizations, und beinhalten AWS Systems Manager. Weitere Informationen finden Sie hier:

  - Was ist AWS CodeBuild? im CodeBuild Benutzerhandbuch.
  - Was ist AWS Organizations? im Benutzerhandbuch für Organisationen.
  - Was ist AWS Systems Manager? im Systems Manager-Benutzerhandbuch.

- Veraltete Version von Account Factory

  Wenn Sie auf ein Problem stoßen und glauben, dass das Problem ein Bug ist, stellen Sie sicher, dass Sie die neueste Version von Account Factory haben. Weitere Informationen finden Sie unter Aktualisieren der Account Factory-Version.

- Lokale Änderungen wurden am Account Factory-Quellcode vorgenommen

  Account Factory ist ein Open-Source-Projekt. AWS Control Tower unterstützt den Account Factory-Kerncode. Wenn Sie eine lokale Änderung am Account Factory-Kerncode vornehmen, unterstützt AWS Control Tower Ihre Account Factory-Bereitstellung nur nach bestem Bemühen.

- Ungenügende Account Factory-Rollenberechtigungen

  Account Factory erstellt IAM-Rollen und -Richtlinien, um die Bereitstellung und Anpassung von Fremdkonten zu verwalten. Wenn Sie diese Rollen oder Richtlinien ändern, kann die Account Factory-Pipeline möglicherweise bestimmte Aktionen nicht ausführen. Weitere Informationen finden Sie unter Erforderliche Rollen.

- Die Konto-Repositorys wurden nicht richtig gefüllt

  Stellen Sie sicher, dass Sie die Schritte nach der Bereitstellung befolgen, bevor Sie Konten bereitstellen.

- Es wird keine Abweichung festgestellt, nachdem die Organisationseinheit manuell geändert wurde

  > **Note**
  >
  > AWS Control Tower erkennt Abweichungen automatisch. Informationen zur Behebung von Abweichungen finden Sie unter Drift in AWS Control Tower erkennen und beheben.

  Eine Abweichung wird nicht erkannt, wenn die Organisationseinheit (OU) manuell geändert wird. Das liegt an der ereignisgesteuerten Natur von Account Factory. Wenn eine Kontoanfrage eingereicht wird, handelt es sich bei der von Terraform verwalteten Ressource um einen Amazon DynamoDB-Artikel, nicht um einen direkten Account. Nachdem ein Element geändert wurde, wird die Anfrage in eine Warteschlange gestellt, wo AWS Control Tower sie über Service Catalog (den Service, der die Kontodetails verwaltet) verarbeitet. Wenn Sie die Organisationseinheit manuell ändern, wird keine Abweichung festgestellt, da sich die Kontoanfrage nicht geändert hat.

Probleme im Zusammenhang mit dem Konto provisioning/registration

- Kontoanfrage (E-Mail address/name) ist bereits vorhanden

  Das Problem führt in der Regel dazu, dass das Service Catalog-Produkt während der Bereitstellung oder als `ConditionalCheckFailedException` ausfällt.

  Weitere Informationen zu dem Problem finden Sie, indem Sie einen der folgenden Schritte ausführen:

  - Überprüfen Sie Ihre Terraform- oder CloudWatch Logs-Protokollgruppen.
  - Überprüfen Sie die Fehler, die an das Amazon SNS-Thema gemeldet werden. `aft-failure-notifications`
- Falsch formatierte Kontoanfrage

  Stellen Sie sicher, dass Ihre Kontoanfrage dem erwarteten Schema entspricht. Beispiele finden Sie unter https://github.com/aws-ia/terraform-aws-control_tower_account_factory/tree/main/sources/aft-customizations-repos/aft-account-request/examples terraform-aws-control_tower_account_factory on. GitHub
- AWS Die Ressourcenkontingente der Organisation wurden überschritten

  Stellen Sie sicher, dass Ihre Kontoanfrage die AWS Organizations Ressourcenkontingente nicht überschreitet. Weitere Informationen finden Sie unter Kontingente für AWS Organisationen.

Probleme im Zusammenhang mit dem Aufrufen von Anpassungen

- Das Zielkonto ist nicht in Account Factory integriert

  Vergewissern Sie sich, dass alle Konten, die in einer Anpassungsanfrage enthalten sind, in Account Factory integriert wurden. Weitere Informationen findest du unter Bestehendes Konto aktualisieren.
- Das Konto, auf das die Anpassungsanforderung abzielt, ist in der DynamoDB-Tabelle**`aft-request-metadata`**, aber nicht im Kontoanforderungs-Repository vorhanden

  Formatieren Sie Ihre Anfrage zum Aufruf der Anpassung so, dass das Konto, das die Störung verursacht, ausgeschlossen wird, indem Sie einen der folgenden Schritte ausführen:

  - Löschen Sie in der DynamoDB-Tabelle den Eintrag`aft-request-metadata`, der auf das Konto verweist, das sich nicht mehr in Ihrem Kontoanforderungs-Repository befindet.

  - „Alle“ werden nicht als Ziel verwendet.
  - Es zielt nicht auf die Organisationseinheit ab, zu der das Konto gehört.
  - Es zielt nicht direkt auf das Konto ab.
- Falsches Token für HCP Terraform verwendet

  Stellen Sie sicher, dass Sie das richtige Token eingerichtet haben. HCP Terraform unterstützt nur teambasierte Token, keine organisationsbasierten Token.
- Konto konnte nicht erstellt werden, bevor die Pipeline für Kontoanpassungen erstellt wurde; Konto kann nicht angepasst werden

  Nehmen Sie im Repository für Kontoanfragen eine Änderung an der Kontospezifikation vor. Wenn Sie eine Änderung vornehmen, z. B. einen Tag-Wert für ein Konto ändern, folgt Account Factory dem Pfad, der versucht, die Pipeline zu erstellen, auch wenn die Pipeline nicht existiert.

Probleme im Zusammenhang mit dem Workflow zur Kontoanpassung

Wenn Sie Probleme im Zusammenhang mit dem Workflow für Kontoanpassungen haben, stellen Sie sicher, dass Ihre Version von AFT 1.8.0 oder höher ist und dass Sie alle Instanzen kontobezogener Metadaten aus Ihrer DynamoDB-Anforderungstabelle löschen.

Informationen zur AFT-Version 1.8.0 finden Sie unter Version 1.8.0 am. https://github.com/aws-ia/terraform-aws-control_tower_account_factory/releases/tag/1.8.0 GitHub

Informationen darüber, wie Sie Ihre Version von AFT überprüfen und aktualisieren können, finden Sie unter den folgenden Links:

- Überprüfen Sie die AFT-Version
- Aktualisieren Sie die AFT-Version

Sie können Anpassungsanfragen auch verfolgen und Fehler beheben, indem Sie Amazon CloudWatch Logs Insights-Abfragen verwenden, um Protokolle zu filtern, die Ihr Zielkonto und Ihre Anpassungsanforderungs-IDs enthalten. Weitere Informationen finden Sie unter Problembehandlung bei der Ablaufverfolgung von Anfragen zur Anpassung von AFT-Konten.

Abweichungen im AWS Control Tower erkennen und beheben

Die Identifizierung und Behebung von Abweichungen ist eine reguläre Betriebsaufgabe für Administratoren von AWS Control Tower Tower-Managementkonten. Die Behebung von Abweichungen trägt dazu bei, dass Sie die Governance-Anforderungen einhalten.

Wenn Sie Ihre landing zone erstellen, entsprechen die landing zone und alle Organisationseinheiten (OUs), Konten und Ressourcen den Governance-Regeln, die durch die von Ihnen ausgewählten Kontrollen durchgesetzt werden. Wenn Sie und Ihre Organisationsmitglieder die landing zone nutzen, kann es zu Änderungen dieses Compliance-Status kommen. Einige Änderungen können versehentlich oder absichtlich vorgenommen werden, um auf zeitkritische Betriebsereignisse zu reagieren.

Sie können mithilfe der Abweichungserkennung feststellen, für welche Ressourcen Änderungen oder Konfigurationsaktualisierungen erforderlich sind.

Drift erkennen

AWS Control Tower erkennt Drift automatisch. Um Abweichungen zu erkennen, benötigt die `AWSControlTowerAdmin` Rolle dauerhaften Zugriff auf Ihr Verwaltungskonto, sodass AWS Control Tower schreibgeschützte API-Aufrufe an ausführen kann. AWS Organizations Diese API-Aufrufe werden als AWS CloudTrail Ereignisse angezeigt.

Abweichungen für ein Mitgliedskonto werden in den Amazon Simple Notification Service (Amazon SNS) -Benachrichtigungen angezeigt, die im Auditkonto zusammengefasst sind. Benachrichtigungen in jedem Mitgliedskonto senden Benachrichtigungen an ein lokales Amazon SNS SNS-Thema und an eine Lambda-Funktion.

> **Note**
>
> Wenn die automatische Registrierung für Konten in den Einstellungen aktiviert ist, sind diese SNS-Benachrichtigungen nicht verfügbar.

Bei Kontrollen, die Teil von AWS Security Hub CSPM Service-Managed Standard: AWS Control Tower sind, wird Drift auf den Seiten Konto und Kontodetails in der AWS Control Tower Tower-Konsole sowie in Form einer Amazon SNS SNS-Benachrichtigung angezeigt.

Administratoren von Mitgliedskonten können (und sollten als bewährte Methode) die SNS-Abweichungsbenachrichtigungen für bestimmte Konten abonnieren. Das `aws-controltower-AggregateSecurityNotifications` SNS-Thema bietet beispielsweise Drift-Benachrichtigungen. Die AWS Control Tower Tower-Konsole zeigt den Administratoren des Verwaltungskontos an, wenn eine Abweichung aufgetreten ist. Weitere Informationen zu SNS-Themen zur Erkennung und Benachrichtigung von Abweichungen finden Sie unter Drift-Prävention und Benachrichtigung.

Deduplizierung von Drift-Benachrichtigungen

Wenn dieselbe Art von Drift mehrmals auf derselben Gruppe von Ressourcen auftritt, sendet AWS Control Tower eine SNS-Benachrichtigung nur für die erste Drift-Instanz. Wenn AWS Control Tower feststellt, dass dieser Drift behoben wurde, sendet er nur dann eine weitere Benachrichtigung, wenn die Drift für diese identischen Ressourcen erneut auftritt.

Beispiel: SCP-Drift wird auf folgende Weise behandelt

- Wenn Sie dasselbe verwaltete SCP mehrmals ändern, erhalten Sie eine Benachrichtigung, wenn Sie es zum ersten Mal ändern.
- Wenn Sie ein verwaltetes SCP ändern, dann Abweichungen beheben und es dann erneut ändern, erhalten Sie zwei Benachrichtigungen.

Arten von Kontoverschiebungen

- Konto wurde zwischen Organisationseinheiten verschoben (siehe Vererbungsabweichung bei aktivierten Baselinesund Vererbungsabweichung bei aktivierten Steuerelementen)
- Konto wurde aus der Organisation entfernt

> **Note**
>
> Wenn Sie ein Konto von einer Organisationseinheit in eine andere verschieben, werden die Steuerelemente der vorherigen Organisationseinheit nicht entfernt. Wenn Sie eine neue Hook-basierte Steuerung auf der Ziel-OU aktivieren, wird die alte Die Hook-basierte Steuerung wird aus dem Konto entfernt und durch die neue Steuerung ersetzt. Mit SCPs und

AWS Config Regeln implementierte Kontrollen müssen immer manuell entfernt werden, wenn ein Konto die Organisationseinheit wechselt.

Beispiele für politische Abweichungen

- SCP wurde aktualisiert
- SCP wurde von OU getrennt

Weitere Informationen finden Sie unter Arten von Abweichungen in der Unternehmensführung.

Meinungsverschiedenheiten

Sie können den Drift-Status für Ihre Konten und Organisationseinheiten über die Konsole oder APIs einsehen und feststellen, wann Konto- und OU-Konfigurationen verändert oder nicht mehr synchron sind. Der Drift-Status wird auch mit SNS-Nachrichten übermittelt. Weitere Informationen zum Empfang dieser SNS-Nachrichten finden Sie unter Anleitung zum Abonnieren von SNS-Themen.

Rufen Sie die Organisationsseite auf und wählen Sie dann die Organisationseinheiten oder Konten aus, die Sie überprüfen möchten, um den Status der Organisationseinheiten und Konten in der Konsole einzusehen.

Rufen Sie die `ListEnabledBaselines`API auf, um den Drift-Status für OUs und Konten programmgesteuert anzuzeigen, um den Status Ihrer aktivierten Baselines einzusehen. Verwenden Sie das Flag, um den Status einzelner Konten programmgesteuert mit der API anzuzeigen. `ListEnabledBaselines includeChildren` Sie können nach diesen Status filtern und nur die Konten und Organisationseinheiten sehen, die Ihre Aufmerksamkeit erfordern.

> **Note**
>
> AWS Control Tower generiert ein Lebenszyklusereignis, wenn jeder Drift-Korrekturvorgang abgeschlossen ist.

Behebung von Abweichungen

Die Erkennung erfolgt zwar automatisch, die Schritte zur Behebung von Abweichungen müssen jedoch manuell über die Konsole oder über die APIs ausgeführt werden. (Außer in bestimmten Fällen, in denen die automatische Registrierung für Konten aktiviert ist, die verschoben wurden.)

Sie können beispielsweise Abweichungen von Richtlinien für Steuerelemente programmgesteuert beheben, indem Sie die API aufrufen. `ResetEnabledControl`

Um Abweichungen bei den Konfigurationsbasislinien für eine OU zu beheben, können Sie Re-register OU in der Konsole auswählen. Wenn die Abweichung durch ein einzelnes Konto verursacht wird, können Sie in der Konsole die Option Konto aktualisieren auswählen. Um die Basisabweichung mit den APIs zu beheben, können Sie die `ResetEnabledBaseline`API auf der Organisationseinheit aufrufen.

Zusammenfassung

- Viele Arten von Abweichungen können auf der Seite mit den Einstellungen für die Landingzone behoben werden. Sie können im Abschnitt Versionen auf die Schaltfläche „Zurücksetzen“ klicken, um diese Arten von Abweichungen zu beheben.
- Wenn Ihre OU weniger als 1000 Konten hat, können Sie Drift in Account Factory Provisioned Accounts (SCP-Drift) beheben, indem Re-registerSie OU auf der Organisationsseite oder der Seite mit den OU-Details auswählen.
- Möglicherweise können Sie Kontoabweichungen beheben, indem Sie Mitgliedskonto wurde verschoben beispielsweise ein einzelnes Konto aktualisieren. Weitere Informationen finden Sie unter Aktualisiere das Konto in der Konsole.
- Bei Steuerungen können viele Arten von Abweichungen durch einen Aufruf der `ResetEnabledControl`API behoben werden.
- Basisabweichungen bei Organisationseinheiten und Konten können behoben werden, indem Sie die `ResetEnabledBaseline`API aufrufen oder indem Re-register Sie in der AWS Control Tower Tower-Konsole OU oder Konto aktualisieren auswählen.
- Um Vererbungsabweichungen zu beheben, die auftreten, wenn Konten zwischen Organisationseinheiten verschoben werden, können Sie die Funktion zur automatischen Registrierung aktivieren. Wenn die automatische Registrierung aktiviert ist, behebt AWS Control Tower automatisch Vererbungsabweichungen, indem die Basisressourcen und Kontrollkonfigurationen von der Ziel-OU auf das verschobene Konto angewendet werden.

Sie können die automatische Registrierung auf der Seite mit den Landingzone-Einstellungen in der Konsole aktivieren oder indem Sie die **`UpdateLandingZone`**API aufrufen, wobei der **`RemediationType`** Parameter auf Inheritance Drift gesetzt ist. Weitere Informationen finden Sie unter Konten mit automatischer Registrierung verschieben und registrieren.

⚠ Wenn Sie Maßnahmen ergreifen, um Drift in einer landing zone Zone-Version zu beheben, hängt das Verhalten von Ihrer aktuellen Version ab.

- Wenn Sie die Landezone-Version 3.1 oder höher verwenden, können Sie „Aktualisieren“ wählen, um Ihre Landezonenkonfiguration zu ändern, ohne die Versionen zu aktualisieren, oder „Zurücksetzen“ wählen, um Ihre gespeicherten Konfigurationen erneut auf Ihre Drifting-Landing-Zone-Ressourcen anzuwenden. Die Drift wurde im Rahmen des Aktualisierungsprozesses behoben.
- Wenn Sie eine landing zone Zone-Version vor 3.1 verwenden, können Sie Reset nicht wählen. Sie müssen Update wählen und Ihre landing zone auf mindestens Version 3.1 aktualisieren.

Überlegungen zu Drift- und Policy-Scans

AWS Control Tower scannt täglich Ihre verwalteten SCPs, RCPs und deklarativen Richtlinien, um sicherzustellen, dass die entsprechenden Kontrollen korrekt angewendet werden und dass sie nicht verändert wurden. Um diese Ressourcen abzurufen und zu überprüfen, ruft AWS Control Tower in Ihrem Namen AWS Organizations an und verwendet dabei eine Rolle in Ihrem Verwaltungskonto.

Wenn bei einem AWS Control Tower Tower-Scan Abweichungen festgestellt werden, erhalten Sie eine Benachrichtigung. AWS Control Tower sendet nur eine Benachrichtigung pro Drift-Problem. Wenn sich Ihre landing zone also bereits im Drift-Zustand befindet, erhalten Sie keine weiteren Benachrichtigungen, es sei denn, es wird ein neuer Drift-Artikel gefunden.

AWS Organizations schränkt ein, wie oft die einzelnen APIs aufgerufen werden können. Dieses Limit wird in Transaktionen pro Sekunde (TPS) ausgedrückt und wird als TPS-Limit, Drosselungsrate oder API-Anforderungsrate bezeichnet. Wenn AWS Control Tower Ihre SCPs, RCPs und deklarativen Richtlinien durch Aufrufe prüft AWS Organizations, werden die API-Aufrufe, die AWS Control Tower durchführt, auf Ihr TPS-Limit angerechnet, da AWS Control Tower das Verwaltungskonto für die Aufrufe verwendet.

In seltenen Fällen kann dieses Limit erreicht werden, wenn Sie dieselben APIs wiederholt aufrufen, sei es über eine Drittanbieterlösung oder ein von Ihnen geschriebenes benutzerdefiniertes Skript. Wenn Sie und AWS Control Tower beispielsweise dieselben AWS Organizations APIs zum gleichen Zeitpunkt (innerhalb von 1 Sekunde) aufrufen und die TPS-Grenzwerte erreicht sind, werden nachfolgende Aufrufe gedrosselt. Das heißt, diese Aufrufe geben einen Fehler zurück wie. `Rate exceeded`

Wenn eine API-Anforderungsrate überschritten wird

- Wenn AWS Control Tower das Limit erreicht und gedrosselt wird, unterbrechen wir die Ausführung des Audits und setzen es zu einem späteren Zeitpunkt fort.
- Wenn Ihr Workload das Limit erreicht und gedrosselt wird, kann das Ergebnis, je nachdem, wie der Workload konfiguriert ist, von einer leichten Latenz bis hin zu einem schwerwiegenden Fehler in der Arbeitslast reichen. Dieser Grenzfall ist etwas, das Sie beachten sollten.

Ein täglicher SCP-Scan besteht aus

1. Ihre kürzlich aktiven Organisationseinheiten werden abgerufen.
2. Für jede registrierte OU werden alle von AWS Control Tower verwalteten SCPs abgerufen, die an die OU angehängt sind. Verwaltete SCPs haben Identifikatoren, die mit beginnen. `aws-guardrails`
3. Für jede präventive Kontrolle, die auf der OU aktiviert ist, wird überprüft, ob die Richtlinienerklärung der Kontrolle in den verwalteten SCPs der OU enthalten ist.

Eine Organisationseinheit kann über einen oder mehrere verwaltete SCPs verfügen.

Arten von Abweichungen, die sofort behoben werden müssen

Die meisten Arten von Abweichungen können von Administratoren behoben werden. Einige Arten von Abweichungen müssen sofort behoben werden, einschließlich der Löschung einer Organisationseinheit, die für die AWS Control Tower Tower-Landezone erforderlich ist. Hier sind einige Beispiele für größere Abweichungen, die Sie vielleicht vermeiden möchten:

- Löschen Sie die Sicherheits-OU nicht: Die Organisationseinheit, die ursprünglich bei der Einrichtung der landing zone durch AWS Control Tower Security benannt wurde, sollte nicht gelöscht werden. Wenn du es löschst, wird eine Fehlermeldung angezeigt, in der du aufgefordert

wirst, die landing zone sofort zurückzusetzen. Sie können in AWS Control Tower keine weiteren Aktionen ausführen, bis der Reset abgeschlossen ist.

- Löschen Sie keine erforderlichen Rollen: AWS Control Tower überprüft bestimmte AWS Identity and Access Management (IAM-) Rollen, wenn Sie sich bei der Konsole anmelden, auf IAM-Rollendrift. Wenn diese Rollen fehlen oder nicht zugänglich sind, wird eine Fehlerseite angezeigt, auf der Sie aufgefordert werden, Ihre landing zone zurückzusetzen. Diese Rollen sind. `AWSControlTowerAdmin` `AWSControlTowerCloudTrailRole` `AWSControlTowerStackSetRole`

  Weitere Informationen zu diesen Rollen finden Sie unter Für die Verwendung der AWS Control Tower-Konsole sind Berechtigungen erforderlich.
- Löschen Sie nicht alle zusätzlichen Organisationseinheiten: Für den Betrieb von AWS Control Tower ist mindestens eine zusätzliche Organisationseinheit erforderlich, es muss sich jedoch nicht um die Sandbox-Organisationseinheit handeln.
- Nicht gemeinsam genutzte Konten entfernen: Wenn Sie gemeinsam genutzte Konten mit der AWS Organizations Konsole oder den APIs aus den Foundation-Organisationseinheiten entfernen, z. B. wenn Sie das Protokollierungskonto aus der Sicherheits-OU entfernen. Durch das Verschieben dieser Konten kommt es zu einer Art Fehlverhalten beim Verschieben von Konten, das behoben werden muss. Um diese Art von Drift zu beheben, müssen Sie die landing zone aktualisieren.

> **Note**
>
> Es hat sich bewährt, diese gemeinsam genutzten Konten nicht aus der Foundational OU zu verschieben.

Reparierbare Änderungen an Ressourcen

Im Folgenden finden Sie eine Liste der Änderungen an den AWS Control Tower Tower-Ressourcen, die zulässig sind, obwohl sie zu behebbaren Abweichungen führen. Die Ergebnisse dieser erlaubten Operationen können in der AWS Control Tower Tower-Konsole eingesehen werden, obwohl möglicherweise eine Aktualisierung erforderlich ist.

Weitere Informationen zur Behebung der daraus resultierenden Abweichung finden Sie unter Ressourcen außerhalb von AWS Control Tower verwalten.

Änderungen, die außerhalb der AWS Control Tower Tower-Konsole zulässig sind

- Ändern Sie den Namen einer registrierten Organisationseinheit.
- Ändern Sie den Namen der Sicherheits-OU.
- Ändern Sie den Namen von Mitgliedskonten in Organisationseinheiten, die nicht zu den Grundlagen gehören.
- Löschen Sie eine Organisationseinheit, die nicht zu den Grundlagen gehört.
- Löscht ein registriertes Konto aus einer Organisationseinheit, die nicht zu den Grundlagen gehört.
- Ändern Sie die E-Mail-Adresse eines gemeinsam genutzten Kontos in der Security OU.
- Ändern Sie die E-Mail-Adresse eines Mitgliedskontos in einer registrierten Organisationseinheit.

> **Note**
>
> Das Verschieben von Konten zwischen Organisationseinheiten gilt als Drift und muss gelöst werden.

Drift und Bereitstellung neuer Konten

Wenn sich Ihre landing zone im Drift-Zustand befindet, funktioniert die Funktion „Konto registrieren“ in AWS Control Tower nicht. In diesem Fall müssen Sie neue Konten über AWS Service Catalog einrichten. Detaillierte Anweisungen finden Sie unter Stellen Sie Konten in der Service Catalog-Konsole mit Account Factory bereit.

Insbesondere wenn Sie mithilfe des Service Catalog bestimmte Änderungen an Ihren Konten vorgenommen haben, z. B. den Namen Ihres Portfolios geändert haben, funktioniert die Funktion Konto registrieren nicht.

Arten von Abweichungen in der Unternehmensführung

Abweichungen in der Unternehmensführung, auch als organisatorische Drift bezeichnet, treten auf, wenn OUs, SCPs und Mitgliedskonten geändert oder aktualisiert werden. Folgende Arten von Governance-Abweichungen können in AWS Control Tower erkannt werden:

- Veränderungen bei der Verwaltung von Konten und Organisationseinheiten

- Drift in die Landezone
- Kontrolldrift bei Kontrollen ohne SCP
- Vererbungsabweichung bei Ausgangswerten und Kontrollen

In den nächsten Abschnitten finden Sie detaillierte Informationen zu diesen Arten von Abweichungen, die AWS Control Tower meldet, und zu deren Behebung.

> **Note**
>
> AWS Control Tower beendet das Senden von Drift-Benachrichtigungen an das SNS-Thema für Kunden mit dem Status LZ4.0 + und beginnt stattdessen, Drift-Benachrichtigungen EventBridge an das Verwaltungskonto zu senden. Beispiele für Ereignisse und Anleitungen zum Empfang von Drift-Benachrichtigungen EventBridge finden Sie im nachfolgenden Abschnitt zur EventBridge Erstellung.

Änderungen bei der Verwaltung von Konten und Organisationseinheiten

- Mitgliedskonto wurde verschoben
- Mitgliedskonto wurde entfernt
- Ungeplantes Update auf Managed SCP
- SCP wurde von der verwalteten Organisationseinheit getrennt

Drift in die Landezone

Eine andere Art von Drift ist die Landezonendrift, die über das Verwaltungskonto ermittelt werden kann. Ein Drift in der Landezone besteht aus einer Verschiebung der IAM-Rollen oder jeder Art von organisatorischer Drift, die sich speziell auf grundlegende Organisationseinheiten und gemeinsam genutzte Konten auswirkt.

- Die grundlegende Organisationseinheit wurde gelöscht
- Vertrauenswürdiger Zugriff deaktiviert

Ein Sonderfall von Landezonendrift ist die Rollendrift, die erkannt wird, wenn eine benötigte Rolle nicht verfügbar ist. Wenn diese Art von Abweichung auftritt, zeigt die Konsole eine Warnseite und einige Anweisungen zur Wiederherstellung der Rolle an. Ihre landing zone ist nicht verfügbar, bis der

Rollenwechsel behoben ist. Weitere Informationen zur Rollenverschiebung finden Sie im Abschnitt Erforderliche Rollen nicht löschenArten von Abweichungen, die sofort behoben werden müssen.

Kontrollabweichung bei Nicht-SCP-Kontrollen

AWS Control Tower meldet Kontrollabweichungen in Bezug auf Kontrollen, die mit Resource Control Policies (RCPs), deklarativen Richtlinien und Kontrollen implementiert wurden, die Teil des AWS Security Hub CSPM Service-managed Standards sind: AWS Control Tower.

- Security Hub CSPM — Drift bei der Steuerung
- Kontrollieren Sie die Abweichung der Richtlinien

Abweichungen bei der Vererbung von Baselines und Kontrollen

- Basisabweichung aktiviert

  Wenn sich die Basiskonfigurationen auf einem Mitgliedskonto von denen unterscheiden, die auf die übergeordnete Organisationseinheit angewendet wurden, meldet AWS Control Tower eine Vererbungsabweichung für aktivierte Baselines (Ressourcenkonfigurationen) auf diesen OUs und Konten. Weitere Informationen zu Baselines finden Sie unter Typen von Baselines.

  - Vererbungsabweichung bei aktivierten Baselines
- Control Drift aktiviert

  Wenn sich die aktivierten Kontrollkonfigurationen auf einem Mitgliedskonto von denen unterscheiden, die auf die übergeordnete Organisationseinheit angewendet wurden, meldet AWS Control Tower eine Vererbungsabweichung für aktivierte Kontrollen auf diesen Organisationseinheiten und Konten.

  - Vererbungsabweichung bei aktivierten Steuerelementen

Abweichung, die nicht gemeldet wird

- AWS Control Tower sucht nicht nach Abweichungen in Bezug auf andere Services, die mit dem Verwaltungskonto funktionieren AWS CloudTrail, einschließlich Amazon CloudWatch, IAM Identity Center CloudFormation AWS Config,, usw.
- AWS Control Tower erkennt keine Ressourcendrift oder andere Arten von Drift, die auftreten können, wenn Sie die in einer Baseline enthaltenen Ressourcen ändern.

Mitgliedskonto wurde verschoben

> **Note**
>
> Für Kunden mit LZ 4.0+ sendet AWS Control Tower keine Benachrichtigungen über Kontoverschiebungen für Account Factory Factory-Konten ohne. AWSControlTowerBaseline

Diese Art von Abweichung tritt eher auf dem Konto als auf der Organisationseinheit auf. Diese Art von Abweichung kann auftreten, wenn ein AWS Control Tower Tower-Mitgliedskonto, das Auditkonto oder das Protokollarchiv-Konto von einer registrierten AWS Control Tower Tower-Organisationseinheit in eine andere Organisationseinheit verschoben wird. In vielen Fällen können Sie diese Art von Abweichung vermeiden, wenn Sie die automatische Registrierung für Konten auf der Seite Einstellungen aktivieren. Weitere Details finden Sie unter Konten mit automatischer Registrierung verschieben und registrieren.

Im Folgenden finden Sie ein Beispiel für eine Drift-Benachrichtigung, wenn diese Art von Abweichung erkannt wird.

```
{
  "Message" : "AWS Control Tower has detected that your member account 'account-
email@amazon.com (012345678909)' has been moved from organizational unit 'Sandbox
 (ou-0123-eEXAMPLE)' to 'Security (ou-3210-1EXAMPLE)'. For more information, including
 steps to resolve this issue, see 'https://docs.aws.amazon.com/console/controltower/
move-account'",
  "ManagementAccountId" : "012345678912",
  "OrganizationId" : "o-123EXAMPLE",
  "DriftType" : "ACCOUNT_MOVED_BETWEEN_OUS",
  "RemediationStep" : "Re-register this organizational unit (OU), or if the OU has more
 than 1000 accounts, you must update the provisioned product in Account Factory.",
  "AccountId" : "012345678909",
  "SourceId" : "012345678909",
  "DestinationId" : "ou-3210-1EXAMPLE"
}
```

Lösungen

Wenn diese Art von Abweichung bei einem von Account Factory bereitgestellten Konto in einer Organisationseinheit mit bis zu 1000 Konten auftritt, können Sie sie wie folgt beheben:

- Navigieren Sie in der AWS Control Tower Tower-Konsole zur Seite Organisation, wählen Sie das Konto aus und wählen Sie oben rechts Konto aktualisieren (schnellste Option für einzelne Konten).
- Navigieren Sie in der AWS Control Tower Tower-Konsole zur Organisationsseite und wählen Re-registerSie dann die Organisationseinheit aus, die das Konto enthält (schnellste Option für mehrere Konten). Weitere Informationen finden Sie unter Registrieren Sie eine bestehende Organisationseinheit bei AWS Control Tower.
- Aktualisierung des bereitgestellten Produkts in Account Factory. Weitere Informationen finden Sie unter Konten mit AWS Control Tower aktualisieren und verschieben.

> **Note**
>
> Wenn Sie mehrere individuelle Konten aktualisieren müssen, finden Sie auch diese Methode zum Durchführen von Aktualisierungen mit einem Skript:Konten mithilfe von Automatisierung bereitstellen und aktualisieren.

- Wenn diese Art von Abweichung in einer Organisationseinheit mit mehr als 1000 Konten auftritt, kann die Auflösung der Abweichung davon abhängen, welcher Kontotyp verschoben wurde, wie in den nächsten Absätzen erläutert. Weitere Informationen finden Sie unter Aktualisiere deine landing zone.
  - Wenn ein von Account Factory bereitgestelltes Konto verschoben wird — In einer OU mit weniger als 1000 Konten können Sie die Kontoverschiebung beheben, indem Sie das bereitgestellte Produkt in Account Factory aktualisieren, die OU erneut registrieren oder Ihre landing zone aktualisieren.

    In einer Organisationseinheit mit mehr als 1000 Konten müssen Sie die Abweichung beheben, indem Sie für jedes verschobene Konto eine Aktualisierung vornehmen, entweder über die AWS Control Tower Tower-Konsole oder das bereitgestellte Produkt, da die Re-register OU das Update nicht durchführt. Weitere Informationen finden Sie unter Konten mit AWS Control Tower aktualisieren und verschieben.
  - Wenn ein geteiltes Konto verschoben wird — Sie können die Abweichung vom Verschieben des Audit- oder Protokollarchiv-Kontos beheben, indem Sie Ihre landing zone aktualisieren. Weitere Informationen finden Sie unter Aktualisiere deine landing zone.

⚠ Veralteter Feldname

Der Feldname `MasterAccountID` wurde geändert, sodass er den Richtlinien `ManagementAccountID` entspricht AWS . Der alte Name ist veraltet. Seit 2022 funktionieren Skripten, die den veralteten Feldnamen enthalten, nicht mehr.

Mitgliedskonto wurde entfernt

Diese Art von Abweichung kann auftreten, wenn ein Mitgliedskonto aus einer registrierten AWS Control Tower Tower-Organisationseinheit entfernt wird. Das folgende Beispiel zeigt die Drift-Benachrichtigung, wenn diese Art von Abweichung erkannt wird.

```
{
  "Message" : "AWS Control Tower has detected that the member account 012345678909 has
 been removed from organization o-123EXAMPLE. For more information, including steps
 to resolve this issue, see 'https://docs.aws.amazon.com/console/controltower/remove-
account'",
  "ManagementAccountId" : "012345678912",
  "OrganizationId" : "o-123EXAMPLE",
  "DriftType" : "ACCOUNT_REMOVED_FROM_ORGANIZATION",
  "RemediationStep" : "Add account to Organization and update Account Factory
 provisioned product",
  "AccountId" : "012345678909"
}
```

Auflösung

- Wenn diese Art von Abweichung in einem Mitgliedskonto auftritt, können Sie die Abweichung beheben, indem Sie das Konto in der AWS Control Tower Tower-Konsole oder in Account Factory aktualisieren. Sie können das Konto beispielsweise über den Account Factory Factory-Update-Assistenten zu einer anderen registrierten Organisationseinheit hinzufügen. Weitere Informationen finden Sie unter Konten mit AWS Control Tower aktualisieren und verschieben.
- Wenn ein gemeinsam genutzter Account aus einer Foundational OU entfernt wird, müssen Sie die Abweichung beheben, indem Sie Ihre landing zone zurücksetzen. Solange dieser Fehler nicht behoben ist, können Sie die AWS Control Tower Tower-Konsole nicht verwenden.
- Weitere Informationen zum Beheben von Abweichungen für Konten und OUs finden Sie unter Wenn Sie Ressourcen außerhalb von AWS Control Tower verwalten.

> **Note**
>
> In Service Catalog wird das von Account Factory bereitgestellte Produkt, das das Konto darstellt, nicht aktualisiert, um das Konto zu entfernen. Stattdessen wird das bereitgestellte Produkt als `TAINTED` und in einem Fehlerzustand angezeigt. Gehen Sie zum Aufräumen zum Service Catalog, wählen Sie das bereitgestellte Produkt aus und klicken Sie dann auf Terminate.

Ungeplantes Update auf Managed SCP

Diese Art von Abweichung kann auftreten, wenn ein SCP für ein Steuerelement in der AWS Organizations Konsole oder programmgesteuert mithilfe des AWS CLI oder eines der AWS-SDKs aktualisiert wird. Im Folgenden finden Sie ein Beispiel für die Drift-Benachrichtigung, wenn diese Art von Abweichung erkannt wird.

```
{
  "Message" : "AWS Control Tower has detected that the managed service control policy
 'aws-guardrails-012345 (p-tEXAMPLE)', attached to the registered organizational unit
 'Security (ou-0123-1EXAMPLE)', has been modified. For more information, including
 steps to resolve this issue, see 'https://docs.aws.amazon.com/console/controltower/
update-scp'",
  "ManagementAccountId" : "012345678912",
  "OrganizationId" : "o-123EXAMPLE",
  "DriftType" : "SCP_UPDATED",
  "RemediationStep" : "Update Control Tower Setup",
  "OrganizationalUnitId" : "ou-0123-1EXAMPLE",
  "PolicyId" : "p-tEXAMPLE"
}
```

Auflösung

Wenn diese Abweichung in einer Organisationseinheit mit bis zu 1000 Konten auftritt, können Sie sie wie folgt beheben:

- Navigieren Sie zur Organisationsseite in der AWS Control Tower Tower-Konsole, um die Organisationseinheit erneut zu registrieren (schnellste Option). Weitere Informationen finden Sie unter Registrieren Sie eine bestehende Organisationseinheit bei AWS Control Tower.

- Aktualisierung Ihrer landing zone (langsamere Option). Weitere Informationen finden Sie unter Aktualisiere deine landing zone.

Wenn diese Art von Abweichung in einer Organisationseinheit mit mehr als 1000 Konten auftritt, beheben Sie das Problem, indem Sie Ihre landing zone aktualisieren. Weitere Informationen finden Sie unter Aktualisiere deine landing zone.

SCP wurde von der verwalteten Organisationseinheit getrennt

Diese Art von Abweichung kann auftreten, wenn ein SCP für eine Steuerung von einer OU getrennt wurde, die von AWS Control Tower verwaltet wird. Dieses Ereignis tritt besonders häufig auf, wenn Sie von außerhalb der AWS Control Tower Tower-Konsole arbeiten. Im Folgenden finden Sie ein Beispiel für eine Drift-Benachrichtigung, wenn diese Art von Drift erkannt wird.

```
{
  "Message" : "AWS Control Tower has detected that the managed service control
 policy 'aws-guardrails-012345 (p-tEXAMPLE)' has been detached from the registered
 organizational unit 'Sandbox (ou-0123-1EXAMPLE)'. For more information, including
 steps to resolve this issue, see 'https://docs.aws.amazon.com/console/controltower/
scp-detached'",
  "ManagementAccountId" : "012345678912",
  "OrganizationId" : "o-123EXAMPLE",
  "DriftType" : "SCP_DETACHED_FROM_OU",
  "RemediationStep" : "Update Control Tower Setup",
  "OrganizationalUnitId" : "ou-0123-1EXAMPLE",
  "PolicyId" : "p-tEXAMPLE"
}
```

Auflösung

Wenn diese Abweichung in einer Organisationseinheit mit bis zu 1000 Konten auftritt, können Sie sie wie folgt beheben:

- Navigieren Sie zur OU in der AWS Control Tower Tower-Konsole, um die OU erneut zu registrieren (schnellste Option). Weitere Informationen finden Sie unter Registrieren Sie eine bestehende Organisationseinheit bei AWS Control Tower.
- Aktualisierung Ihrer landing zone (langsamere Option). Wenn sich die Abweichung auf eine obligatorische Kontrolle auswirkt, erstellt der Aktualisierungsprozess eine neue Service Control

Policy (SCP) und fügt sie der OU hinzu, um die Abweichung zu beheben. Weitere Informationen zum Aktualisieren Ihrer landing zone finden Sie unterAktualisiere deine landing zone.

Wenn diese Art von Abweichung in einer Organisationseinheit mit mehr als 1000 Konten auftritt, beheben Sie das Problem, indem Sie Ihre landing zone aktualisieren. Wenn sich die Abweichung auf eine obligatorische Kontrolle auswirkt, erstellt der Aktualisierungsprozess eine neue Service Control Policy (SCP) und fügt sie der OU hinzu, um die Abweichung zu beheben. Weitere Informationen zum Aktualisieren Ihrer landing zone finden Sie unterAktualisiere deine landing zone.

Die grundlegende Organisationseinheit wurde gelöscht

Diese Art von Abweichung gilt nur für AWS Control Tower Foundational OUs, wie z. B. die Security OU. Es kann vorkommen, wenn eine Foundational OU außerhalb der AWS Control Tower Tower-Konsole gelöscht wird. Grundlegende Organisationseinheiten können nicht verschoben werden, ohne dass es zu einer solchen Abweichung kommt, da das Verschieben einer Organisationseinheit dasselbe ist wie das Löschen und das anschließende Hinzufügen an einer anderen Stelle. Wenn Sie die Abweichung beheben, indem Sie Ihre landing zone aktualisieren, ersetzt AWS Control Tower die Foundational OU am ursprünglichen Standort. Das folgende Beispiel zeigt eine Drift-Benachrichtigung, die Sie möglicherweise erhalten, wenn diese Art von Drift erkannt wird.

```
{
  "Message" : "AWS Control Tower has detected that the registered organizational unit
 'Security (ou-0123-1EXAMPLE)' has been deleted. For more information, including steps
 to resolve this issue, see 'https://docs.aws.amazon.com/console/controltower/delete-
ou'",
  "ManagementAccountId" : "012345678912",
  "OrganizationId" : "o-123EXAMPLE",
  "DriftType" : "ORGANIZATIONAL_UNIT_DELETED",
  "RemediationStep" : "Delete organizational unit in Control Tower",
  "OrganizationalUnitId" : "ou-0123-1EXAMPLE"
}
```

Auflösung

Da diese Abweichung nur bei Foundational OUs auftritt, besteht die Lösung darin, die landing zone zu aktualisieren. Wenn andere Arten von Organisationseinheiten gelöscht werden, wird AWS Control Tower automatisch aktualisiert.

Weitere Informationen zum Beheben von Abweichungen für Konten und OUs finden Sie unter Wenn Sie Ressourcen außerhalb von AWS Control Tower verwalten.

Security Hub CSPM — Drift bei der Steuerung

Diese Art von Abweichung tritt auf, wenn eine Steuerung, die Teil des AWS Security Hub CSPM Service-Managed Standards ist: AWS Control Tower, einen Drift-Status meldet. Der AWS Security Hub CSPM Service selbst meldet keinen Drift-Status für diese Kontrollen. Stattdessen sendet der Service seine Ergebnisse an AWS Control Tower.

Eine Drift bei der Kontrolle des Security Hub CSPM kann auch festgestellt werden, wenn AWS Control Tower seit mehr als 24 Stunden kein Status-Update von Security Hub CSPM erhalten hat. Wenn diese Ergebnisse nicht wie erwartet eingehen, überprüft AWS Control Tower, ob die Kontrolle nicht stimmt. Das folgende Beispiel zeigt eine Drift-Benachrichtigung, die Sie möglicherweise erhalten, wenn diese Art von Abweichung erkannt wird.

```
{
"Message" : "AWS Control Tower has detected that an AWS Security Hub control
 was removed in your account example-account@amazon.com <mailto:example-
account@amazon.com>. The artifact deployed on the target OU and accounts does not match
 the expected template and configuration for the control. This mismatch indicates that
 configuration changes were made outside of AWS Control Tower. For more information,
 view Security Hub standard",
"MasterAccountId" : "123456789XXX",
"ManagementAccountId" : "123456789XXX",
"OrganizationId" : "o-123EXAMPLE",
"DriftType" : "SECURITY_HUB_CONTROL_DISABLED",
"RemediationStep" : "To remediate the issue, Re-register the OU, or remove the control
 and enable it again. If the problem persists, contact AWS support.",
"AccountId" : "7876543219XXX",
"ControlId" : "SH.XXXXXXX.1",
"ControlName" : "EBS snapshots should not be publicly restorable",
"ApiControlIdentifier" : "arn:aws:controltower:us-east-1::control/PYBETSAGNUZB",
"EnabledControlIdentifier": "arn:aws:controltower:us-
east-1::enabledcontrol/<UNIQUE_ID>".
"Region" : "us-east-1"
}
```

Auflösung

Für Organisationseinheiten mit weniger als 1000 Konten besteht die empfohlene Lösung darin, die ResetEnabledControlAPI für das Drifted Control aufzurufen. In der Konsole können Sie Re-registerfür die Organisationseinheit auswählen, wodurch die Steuerung auf den ursprünglichen Zustand zurückgesetzt wird. Alternativ können Sie für jede Organisationseinheit die Steuerung über die Konsole oder die AWS Control Tower Tower-APIs entfernen und wieder aktivieren, wodurch auch die Steuerung zurückgesetzt wird.

Weitere Informationen zum Beheben von Abweichungen für Konten und OUs finden Sie unter Wenn Sie Ressourcen außerhalb von AWS Control Tower verwalten.

Kontrollieren Sie die Abweichung der Richtlinien

Diese Art von Abweichung tritt auf, wenn eine Kontrolle, die mithilfe von Ressourcenkontrollrichtlinien (RCPs) oder deklarativen Richtlinien implementiert wurde, eine Abweichung meldet. Es gibt einen Status von zurück`CONTROL_INEFFECTIVE`, den Sie in der AWS Control Tower Tower-Konsole und in der Drift-Nachricht sehen können. Die Drift-Nachricht für diese Art von Drift beinhaltet auch die `EnabledControlIdentifier` für die betroffene Kontrolle.

Diese Art von Drift wird für SCP-based Kontrollen nicht gemeldet.

Das folgende Beispiel zeigt eine Drift-Benachrichtigung, die Sie möglicherweise erhalten, wenn diese Art von Drift erkannt wird.

```
{
    "Message": "AWS Control Tower detects that a policy it owns was updated
 unexpectedly. This mismatch indicates that configuration changes were made outside of
 AWS Control Tower.",
    "MasterAccountId": "123456789XXX",
    "ManagementAccountId": "123456789XXX",
    "OrganizationId": "o-123EXAMPLE",
    "DriftType": "CONTROL_INEFFECTIVE",
    "RemediationStep": "To remediate the issue, Reset the DRIFTED enabled control if
 permitted or Re-register the OU. If the problem persists, contact AWS support.",
    "TargetIdentifier": "arn:aws:::organizations/o-123456/ou-1234-4567",
    "ControlId": "CT.XXXXXXX.PV.1",
    "ControlName": "EBS snapshots should not be publicly restorable",
    "ApiControlIdentifier": "arn:aws:controlcatalog:::control/<UNIQUE_ID>",
    "EnabledControlIdentifier": "arn:aws:controltower:us-
east-1::enabledcontrol/<UNIQUE_ID>"
```

```
}
```

Auflösung

Die einfachste Lösung für Abweichungen von Kontrollrichtlinien bei RCP-Kontrollen, deklarativen Richtlinienkontrollen und Security Hub-CSPM-Steuerungen, die in AWS Control Tower aktiviert sind, besteht darin, die API aufzurufen. `ResetEnabledControl`

Bei Organisationseinheiten mit weniger als 1000 Konten erfolgt eine weitere Lösung über die Konsole oder API über die Organisationseinheit, wodurch Re-registerdie Steuerung auf den ursprünglichen Zustand zurückgesetzt wird.

Für jede einzelne Organisationseinheit können Sie die Steuerung über die Konsole oder die AWS Control Tower Tower-APIs entfernen und wieder aktivieren, wodurch auch die Steuerung zurückgesetzt wird.

Weitere Informationen zum Beheben von Abweichungen für Konten und OUs finden Sie unter Wenn Sie Ressourcen außerhalb von AWS Control Tower verwalten.

Vertrauenswürdiger Zugriff deaktiviert

Diese Art von Drift gilt für Landezonen im AWS Control Tower. Es tritt auf, wenn Sie den vertrauenswürdigen Zugriff auf AWS Control Tower deaktivieren, AWS Organizations nachdem Sie Ihre AWS Control Tower Tower-Landezone eingerichtet haben.

Wenn der vertrauenswürdige Zugriff deaktiviert ist, empfängt AWS Control Tower keine Änderungsereignisse mehr von AWS Organizations. AWS Control Tower ist darauf angewiesen, dass diese Änderungsereignisse synchronisiert bleiben AWS Organizations. Infolgedessen kann es sein, dass AWS Control Tower organisatorische Änderungen an Konten und Organisationseinheiten übersieht. Aus diesem Grund ist es wichtig, dass Sie jedes Mal, wenn Sie Ihre landing zone aktualisieren, jede Organisationseinheit neu registrieren.

Beispiel: Drift-Benachrichtigung

Im Folgenden finden Sie ein Beispiel für die Drift-Benachrichtigung, die Sie erhalten, wenn diese Art von Abweichung auftritt.

```
{
  "Message" : "AWS Control Tower has detected that trusted access has been disabled in
 AWS Organizations. For more information, including steps to resolve this issue, see
```

```
 https://docs.aws.amazon.com/controltower/latest/userguide/drift.html#drift-trusted-
access-disabled",
  "ManagementAccountId" : "012345678912",
  "OrganizationId" : "o-123EXAMPLE",
  "DriftType" : "TRUSTED_ACCESS_DISABLED",
  "RemediationStep" : "Reset Control Tower landing zone."
}
```

Auflösung

AWS Control Tower benachrichtigt Sie, wenn diese Art von Abweichung in der AWS Control Tower Tower-Konsole auftritt. Die Lösung besteht darin, Ihre AWS Control Tower Tower-Landezone zurückzusetzen. Weitere Informationen finden Sie unter Drift beheben.

Vererbungsabweichung bei aktivierten Baselines

Diese Art von Abweichung kann bei den Organisationseinheiten und Konten von AWS Control Tower auftreten.

Auflösung

AWS Control Tower benachrichtigt Sie, wenn diese Art von Drift auftritt. In fast allen Fällen von Abweichungen bei der Vererbung erhalten Sie eine Benachrichtigung über die Änderung des Mitgliedskontos. Das liegt daran, dass diese Art von Abweichung in der Regel auftritt, wenn ein Konto verschoben wurde oder wenn die Registrierung eines Kontos fehlschlägt.

Abweichungen in der Konsole anzeigen und beheben

In der AWS Control Tower Tower-Konsole können Sie diesen vererbten Drift-Status in der Spalte Baseline State auf der Seite Organizations einsehen. Die Lösung von der Konsole aus erfolgt an Re-registerIhre Organisationseinheit oder „Aktualisieren Sie Ihr Konto“.

Fehler programmgesteuert anzeigen und beheben

Um den Drift-Status programmgesteuert anzuzeigen, können Sie die `ListEnabledBaselines`API aufrufen, um den Status der aktivierten Baselines in Ihren Organisationseinheiten einzusehen. Verwenden Sie das Flag, um den Status einzelner Konten programmgesteuert mit der API anzuzeigen. `ListEnabledBaselines includeChildren`

Sie können diese Art von Abweichung programmgesteuert beheben, indem Sie die API aufrufen. `ResetEnabledBaseline`

Vermeiden Sie Vererbungsabweichungen mit automatischer Registrierung

Um diese Abweichung bei future Kontoverschiebungen zu verhindern, aktivieren Sie die automatische Registrierung. Wenn die automatische Registrierung aktiviert ist, wendet AWS Control Tower die Baselines und Kontrollkonfigurationen der Ziel-OU auf ein verschobenes Konto an, wenn Sie das Konto aktualisieren, um es in eine andere OU zu verschieben. Weitere Informationen finden Sie unter. Konten mit automatischer Registrierung verschieben und registrieren Auto-enrollment behebt keine Basisabweichung, die bereits bei einer vorherigen Bewegung besteht. Verwenden Sie eine der weiter oben in diesem Abschnitt beschriebenen Auflösungsmethoden, um bestehende Abweichungen zu beheben. Sie können die Organisationseinheit erneut registrieren, das Konto aktualisieren oder die `ResetEnabledBaseline` API aufrufen.

Vererbungsabweichung bei aktivierten Steuerelementen

Diese Art von Abweichung kann bei den Organisationseinheiten und Konten von AWS Control Tower auftreten.

Auflösung

AWS Control Tower benachrichtigt Sie, wenn diese Art von Drift auftritt. In fast allen Fällen von Abweichungen bei der Vererbung erhalten Sie eine Benachrichtigung über die Änderung des Mitgliedskontos. Diese Art von Abweichung tritt normalerweise auf, wenn Sie ein Konto zwischen Organisationseinheiten verschieben, während die automatische Registrierung deaktiviert ist. In diesem Fall wendet AWS Control Tower die Kontrollen der Ziel-OU auf das Konto an, entfernt jedoch nicht automatisch die Kontrollen, die das Konto von seiner vorherigen Organisationseinheit übernommen hat. Daher können Detective Controls und Proactive Controls aus der vorherigen Organisationseinheit in einem veränderten Zustand auf dem Konto verbleiben. Präventive Kontrollen unterliegen nicht dieser Art von Vererbungsabweichung.

> **Note**
>
> Sie können diese Vererbungsabweichung nicht beheben, indem Sie das Konto aktualisieren, die Organisationseinheit erneut registrieren oder die `ResetEnabledControl` API aufrufen. Diese Aktionen beheben nur Konfigurationsabweichungen. Sie entfernen kein Steuerelement, das ein verschobenes Konto immer noch von seiner vorherigen Organisationseinheit erbt. Um das übrig gebliebene Steuerelement zu entfernen, müssen Sie es mit der `DisableControl` API deaktivieren, wie in diesem Abschnitt beschrieben.

Drift in der Konsole anzeigen

In der AWS Control Tower Tower-Konsole können Sie sehen, welche aktivierte Steuerung den Status Drifted hat. Diese Informationen werden nur auf der Seite mit den Kontodetails für das betroffene Konto angezeigt. Die Konsole zeigt nicht den `EnabledControlIdentifier` (den ARN des aktivierten Steuerelements) an, den Sie zum Deaktivieren eines Drift-Steuerelements benötigen. Um das zu erhalten`EnabledControlIdentifier`, verwenden Sie die AWS Control Tower API, wie in diesem Abschnitt beschrieben.

Sehen Sie sich Abweichungen an und beheben Sie sie mithilfe der AWS CLI

Um herauszufinden, welche Steuerung für das betroffene Konto geändert wurde, listen Sie die aktivierten Kontrollen für dieses Konto auf. Geben Sie dem Konto die Ziel-ID an und fügen Sie das `--include-children` Kennzeichen hinzu, damit die vererbten Steuerelemente zurückgegeben werden:

```
aws controltower list-enabled-controls --target-identifier <account ARN> --include-
children
```

Suchen Sie in der Ausgabe nach dem aktivierten Steuerelement, dessen `inheritance` Drift-Typ einen `DRIFTED` Status anzeigt. Notieren Sie sich den `arn` Wert dieses aktivierten Steuerelements. Mit diesem Wert deaktivieren Sie `EnabledControlIdentifier` das Steuerelement. Beispiel:

```
{
    "arn": "arn:aws:controltower:<Region>:<management account
 ID>:enabledcontrol/<enabled control ID>",
    "controlIdentifier": "arn:aws:controlcatalog:::control/<control ID>",
    "targetIdentifier": "arn:aws:organizations::<management account
 ID>:account/<organization ID>/<member account ID>",
    "driftStatusSummary": {
        "driftStatus": "DRIFTED",
        "types": {
            "inheritance": { "status": "DRIFTED" },
            "resource": { "status": "IN_SYNC" }
        }
    }
}
```

Um das veränderte Steuerelement zu entfernen, deaktivieren Sie es, indem Sie das `EnabledControlIdentifier` an den `disable-control` folgenden Befehl übergeben:

```
aws controltower disable-control --enabled-control-
identifier <EnabledControlIdentifier>
```

Weitere Informationen finden Sie unter ListEnabledControlsund DisableControlin der AWS Control Tower API-Referenz.

Vermeiden Sie Vererbungsabweichungen mit automatischer Registrierung

Um diese Abweichung bei future Kontoverschiebungen zu verhindern, aktivieren Sie die automatische Registrierung. Weitere Informationen finden Sie unter Konten mit automatischer Registrierung verschieben und registrieren. Wenn die automatische Registrierung aktiviert ist, wendet AWS Control Tower die Baselines und Kontrollkonfigurationen der Ziel-OU auf ein verschobenes Konto an und entfernt die Kontrollen der vorherigen Organisationseinheit. Durch die automatische Registrierung werden jedoch keine Steuerelemente entfernt, die bereits von einer Verschiebung übrig geblieben sind, die vor dem Einschalten vorgenommen wurde. Verwenden Sie die API, um diese Steuerelemente zu entfernen. `DisableControl`

EventBridge Schöpfung

> **Note**
>
> EventBridge ist nur für Kunden mit dem Wert LZ4.0 + aktiviert.

EventBridge Beispielformat für AWS Control Tower

```
{
   "version": "0",
   "id": "cd4d811e-ab12-322b-8255-872ce65b1bc8",
   "detail-type": "Drift Detected",
   "source": "aws.controltower",
   "account": "111122223333",
   "time": "2018-03-22T00:38:11Z",
   "region": "us-east-1",
   "resources": [],
   "detail": {
       "message" : "AWS Control Tower has detected that your member account 'account-
email@amazon.com (012345678909)' has been moved from organizational unit 'Sandbox
```

```
 (ou-0123-eEXAMPLE)' to 'Security (ou-3210-1EXAMPLE)'. For more information, including
 steps to resolve this issue, see 'https://docs.aws.amazon.com/console/controltower/
move-account'",
       "managementAccountId" : "012345678912",
       "organizationId" : "o-123EXAMPLE",
       "driftType" : "ACCOUNT_MOVED_BETWEEN_OUS",
       "remediationStep" : "Re-register this organizational unit (OU), or if the OU has
 more than 1000 accounts, you must update the provisioned product in Account Factory.",

       "accountId" : "012345678909",
       "sourceId" : "012345678909",
       "destinationId" : "ou-3210-1EXAMPLE"
   }
}
```

Anleitung zur Erstellung einer EventBridge Regel für den Empfang von Drift-Benachrichtigungen:

Um eine EventBridge Regel für Drift-Benachrichtigungen zu erstellen

1. Öffnen Sie die EventBridge Amazon-Konsole:
2. Wählen Sie im Navigationsbereich Regeln aus.
3. Wählen Sie Regel erstellen aus.
4. Geben Sie einen Namen und eine Beschreibung für die Regel ein.
5. Bei Regeltyp wählen Sie Regel mit einem Ereignismuster aus.
6. Definieren Sie die Ereignisquelle:
   - Wählen Sie für „Ereignisquelle“ AWS Dienste als Ereignisquelle aus.
   - Wählen Sie für „AWS Servicename“ AWS Control Tower aus.
   - Wählen Sie für „Ereignistyp“ die Option Drift Detected aus
7. Wählen Sie das Ziel aus:
   - Wählen Sie für Zieltypen die Option AWS Service und für Ziel auswählen ein Ziel aus, z. B. ein Drift-Benachrichtigungsthema oder eine Lambda-Funktion. Das Ziel wird ausgelöst, wenn ein Ereignis empfangen wird, das dem in der Regel definierten Ereignismuster entspricht.
   - Geben Sie je nach ausgewähltem Ziel die erforderlichen Konfigurationsdetails an, z. B. den Namen der Lambda-Funktion oder den ARN zum Thema Drift-Benachrichtigung.
8. Überprüfen und erstellen Sie die Regel:

- Überprüfen Sie die Details Ihrer Regel und nehmen Sie alle erforderlichen Änderungen vor.
- Wenn Sie zufrieden sind, klicken Sie auf Regel erstellen, um die neue EventBridge Regel zu speichern.

Nach der Erstellung der Regel beginnt sie mit der Überwachung der angegebenen AWS Control Tower Tower-Ereignisse und löst die ausgewählte Zielaktion aus, wenn Drift-Ereignisse auftreten.

Wenn Sie Ressourcen außerhalb von AWS Control Tower verwalten

AWS Control Tower richtet in Ihrem Namen Konten, Organisationseinheiten und andere Ressourcen ein, aber Sie sind der Eigentümer dieser Ressourcen. Sie können diese Ressourcen innerhalb oder außerhalb des AWS Control Tower ändern. Der häufigste Ort, an dem Ressourcen außerhalb des AWS Control Tower geändert werden, ist die AWS Organizations Konsole. In diesem Thema wird beschrieben, wie Sie Änderungen an AWS Control Tower-Ressourcen abgleichen, wenn Sie die Änderungen außerhalb von AWS Control Tower vornehmen.

Das Umbenennen, Löschen und Verschieben von Ressourcen außerhalb der AWS Control Tower-Konsole führt dazu, dass die Konsole nicht mehr synchronisiert ist. Viele Änderungen können automatisch abgeglichen werden. Bestimmte Änderungen erfordern ein Zurücksetzen Ihrer Landezone, um die in der AWS Control Tower-Konsole angezeigten Informationen zu aktualisieren.

Im Allgemeinen führen Änderungen, die Sie außerhalb der AWS Control Tower-Konsole an den AWS-Control-Tower-Ressourcen vornehmen, in Ihrer Landezone zu einem Zustand, in dem die Abweichungen behoben werden können. Weitere Informationen zu diesen Änderungen finden Sie unter Reparierbare Änderungen an Ressourcen.

Aufgaben, für die ein Zurücksetzen der Landezone erforderlich ist

- Löschen der Sicherheitseinheit (Ein Sonderfall, der nicht leichtfertig erfolgen sollte.)
- Ein geteiltes Konto aus der Security OU entfernen (nicht empfohlen.)
- Aktualisierung, Anhängen oder Trennen eines SCP, der der Security OU zugeordnet ist.

Änderungen, die automatisch vom AWS Control Tower aktualisiert werden

- Ändern der E-Mail-Adresse eines angemeldeten Kontos

- Umbenennen eines angemeldeten Kontos
- Erstellung einer neuen Organisationseinheit (OU) auf oberster Ebene
- Umbenennen einer registrierten OU
- Löschen einer registrierten Organisationseinheit (mit Ausnahme der Sicherheits-OU, für die ein Update erforderlich ist)
- Löschen eines registrierten Kontos (mit Ausnahme eines gemeinsam genutzten Kontos in der Security OU.)

> **Note**
>
> AWS Service Catalog behandelt Änderungen anders als AWS Control Tower. AWS Service Catalog kann zu einer Änderung der Unternehmensführung führen, wenn Ihre Änderungen abgeglichen werden. Weitere Informationen zum Aktualisieren eines bereitgestellten Produkts finden Sie in der Dokumentation unter Aktualisieren bereitgestellter Produkte. AWS Service Catalog

Bezieht sich auf Ressourcen außerhalb von AWS Control Tower

Wenn Sie neue Organisationseinheiten und Konten außerhalb von AWS Control Tower erstellen, unterliegen diese nicht dem AWS Control Tower, auch wenn sie möglicherweise angezeigt werden.

Erstellen einer OU

Organisationseinheiten (OUs), die außerhalb von AWS Control Tower erstellt wurden, werden als nicht registriert bezeichnet. Sie werden auf der Organisationsseite angezeigt, unterliegen jedoch nicht den Kontrollen des AWS Control Tower.

Erstellen eines Kontos

Konten, die außerhalb von AWS Control Tower erstellt wurden, werden als Nicht registriert bezeichnet. Registrierte und nicht registrierte Konten, die zu einer OU gehören, die bei AWS Control Tower registriert ist, werden auf der Seite Organisation angezeigt. Konten, die keiner registrierten OU angehören, können über die Konsole eingeladen werden. AWS Organizations Mit dieser Einladung zum Beitritt wird das Konto nicht im AWS Control Tower registriert und die AWS Control Tower-Governance wird nicht auf das Konto ausgedehnt. Um die Verwaltung zu erweitern, indem Sie

das Konto registrieren, gehen Sie in AWS Control Tower zur Seite Organisation oder Kontodetails und wählen Sie Konto registrieren aus.

Externe Änderung der AWS-Control-Tower-Ressourcennamen

Sie können die Namen Ihrer Organisationseinheiten (OUs) und Konten außerhalb der AWS Control Tower-Konsole ändern. Die Konsole wird automatisch aktualisiert, um diese Änderungen widerzuspiegeln.

Umbenennen einer OU

AWS Organizations In können Sie den Namen einer OU ändern, indem Sie entweder die AWS Organizations API oder die Konsole verwenden. Wenn Sie den Namen einer Organisationseinheit außerhalb von AWS Control Tower ändern, spiegelt die AWS Control Tower-Konsole die Namensänderung automatisch wider. Wenn Sie Ihre Konten jedoch mithilfe von bereitstellen AWS Service Catalog, müssen Sie auch Ihre Landing Zone zurücksetzen, um sicherzustellen, dass AWS Control Tower konsistent bleibt AWS Organizations. Der Reset-Workflow gewährleistet die Konsistenz aller Services für die grundlegenden und zusätzlichen Organisationseinheiten. Sie können diese Art von Abweichung auf der Seite mit den Landing-Zone-Einstellungen beheben. Weitere Informationen findest du im Abschnitt „Drift beheben“ unterAbweichungen im AWS Control Tower erkennen und beheben.

AWS Control Tower zeigt die Namen der Organisationseinheiten auf der Seite Organisation im AWS Control Tower-Dashboard an. Sie können sehen, wann Ihr Vorgang zum Zurücksetzen der Landing Zone erfolgreich war.

Umbenennen eines angemeldeten Kontos

Jedes AWS Konto hat einen Anzeigenamen, der vom Root-Benutzer des Kontos in der AWS Fakturierung und Kostenmanagement Konsole geändert werden kann. Wenn Sie ein Konto umbenennen, das bei AWS Control Tower registriert ist, wird die Namensänderung automatisch in AWS Control Tower übernommen. Weitere Informationen zum Ändern des Kontonamens finden Sie unter Verwaltung eines AWS Kontos im AWS Billing User Guide.

Löschen der Sicherheits-Organisationseinheit

Diese Art von Abweichung ist ein Sonderfall. Wenn Sie die Sicherheitseinheit löschen, wird eine Seite mit einer Fehlermeldung angezeigt, auf der Sie aufgefordert werden, Ihre Landezone zurückzusetzen. Sie müssen Ihre Landing Zone zurücksetzen, bevor Sie weitere Aktionen im AWS Control Tower ausführen können.

- Sie können in der AWS Control Tower-Konsole keine Aktionen ausführen und Sie können keine neuen Konten erstellen, AWS Service Catalog bis das Zurücksetzen abgeschlossen ist.
- Sie können die Seite mit den Einstellungen für die Landing Zone nicht aufrufen, um dort die Schaltfläche Zurücksetzen zu sehen.

In diesem Fall wird beim Zurücksetzen der Landingzone eine neue Sicherheitseinheit erstellt und die beiden gemeinsamen Konten in die neue Sicherheitseinheit verschoben. AWS Control Tower markiert die Konten Log Archive und Audit als verschoben. Derselbe Prozess behebt die Abweichung in diesen Konten.

Wenn Sie entscheiden, dass Sie die Sicherheitseinheit löschen müssen, sollten Sie Folgendes wissen:

Bevor Sie die Sicherheitseinheit löschen können, müssen Sie sicherstellen, dass sie keine Konten enthält. Insbesondere müssen Sie die Konten Log Archive und Audit aus der OU entfernen. Es wird empfohlen, diese Konten in eine andere OU zu verschieben.

> **Note**
>
> Das Löschen Ihrer Sicherheits-OU darf nicht ohne gebührende Überlegung durchgeführt werden. Die Aktion könnte zu Compliance-Bedenken führen, wenn die Protokollierung vorübergehend ausgesetzt wird und einige Kontrollen möglicherweise nicht durchgesetzt werden.

Allgemeine Informationen über Abweichungen finden Sie unter „Beheben einer Abweichung“ in Abweichungen im AWS Control Tower erkennen und beheben.

Ein Konto aus der Sicherheits-OU entfernen

Es wird nicht empfohlen, die gemeinsam genutzten Konten aus Ihrer Organisation zu entfernen oder sie aus der Security OU zu verschieben. Wenn Sie versehentlich ein gemeinsames Konto entfernt haben, können Sie die Schritte zur Problembehebung in diesem Abschnitt befolgen, um das Konto wiederherzustellen.

- Von der AWS Control Tower-Konsole aus: Um den Korrekturprozess zu starten, folgen Sie den halbmanuellen Korrekturschritten. Stellen Sie sicher, dass der Benutzer oder die Rolle, die Sie für den Zugriff auf die AWS Control Tower-Konsole verwenden, über Ausführungsberechtigungen

verfügt. `organizations:InviteAccountToOrganization` Wenn Sie nicht über solche Berechtigungen verfügen, folgen Sie den manuellen Korrekturschritten, die sowohl die AWS Control Tower-Konsole als auch die AWS Organizations Konsole verwenden.

- Ausgehend von der AWS Organizations Konsole: Dieser Korrekturprozess ist ein etwas längerer, vollständig manueller Vorgang. Wenn Sie die Schritte zur manuellen Problembehebung ausführen, wechseln Sie zwischen der AWS Organizations Konsole und der AWS Control Tower-Konsole. Wenn Sie darin arbeiten AWS Organizations, benötigen Sie einen Benutzer oder eine Rolle mit der `AWSOrganizationsFullAccess` verwalteten Richtlinie oder einer gleichwertigen Richtlinie. Wenn Sie in der AWS Control Tower-Konsole arbeiten, benötigen Sie einen Benutzer oder eine Rolle mit der `AWSControlTowerServiceRolePolicy` verwalteten Richtlinie oder einem Äquivalent sowie die Erlaubnis, alle AWS Control Tower-Aktionen auszuführen (Controltower: *).
- Wenn das Konto durch die Abhilfemaßnahmen nicht wiederhergestellt wird, wenden Sie sich an. AWS Support

Die Ergebnisse des Entfernens eines gemeinsamen Kontos über AWS Organizations:

- Das Konto ist nicht mehr durch die obligatorischen Kontrollen von AWS Control Tower mit Service Control Policies (SCPs) geschützt. Ergebnis: Die von AWS Control Tower im Konto erstellten Ressourcen können geändert oder gelöscht werden.
- Das Konto befindet sich nicht mehr unter dem AWS Organizations Verwaltungskonto. Ergebnis: Der Administrator des AWS Organizations Verwaltungskontos hat keinen Einblick mehr in die Ausgaben des Kontos.
- Es wird nicht mehr garantiert, dass das Konto von überwacht wird AWS Config. Ergebnis: Der Administrator des AWS Organizations Verwaltungskontos kann möglicherweise keine Ressourcenänderungen erkennen.
- Das Konto befindet sich nicht mehr in der Organisation. Ergebnis: Aktualisierungen und das Zurücksetzen von AWS Control Tower schlagen fehl.

So stellen Sie ein gemeinsames Konto mithilfe der AWS Control Tower-Konsole wieder her (halbmanuelles Verfahren)

1. Melden Sie sich bei der AWS Control Tower-Konsole unter an https://console.aws.amazon.com/controltower. Sie müssen sich als IAM-Benutzer, Benutzer im IAM Identity Center oder als Rolle mit Ausführungsberechtigungen anmelden. `organizations:InviteAccountToOrganization` Wenn Sie nicht über solche

Berechtigungen verfügen, verwenden Sie das weiter unten in diesem Thema beschriebene manuelle Korrekturverfahren.

2. Wählen Sie auf der Seite Landing Zone Drift erkannt aus, ob Re-Invite das Entfernen eines gemeinsamen Accounts behoben werden soll, indem Sie den gemeinsamen Account erneut in die Organisation einladen. Eine automatisch generierte E-Mail wird an die E-Mail-Adresse für das Konto gesendet.
3. Nehmen Sie die Einladung an, das gemeinsame Konto wieder in die Organisation aufzunehmen. Führen Sie eine der folgenden Aktionen aus:
   - Melde dich bei dem geteilten Konto an, das entfernt wurde, und gehe dann zu https://console.aws.amazon.com/organizations/home #/invites
   - Wenn du Zugriff auf die E-Mail-Nachricht hast, die gesendet wurde, als du das Konto erneut eingeladen hast, melde dich bei dem entfernten Konto an und klicke dann auf den Link in der Nachricht, um direkt zur Kontoeinladung zu gelangen.
   - Wenn das geteilte Konto, das entfernt wurde, keiner anderen Organisation angehört, melde dich bei dem Konto an, öffne die AWS Organizations Konsole und navigiere zu Einladungen.
4. Melden Sie sich erneut beim Verwaltungskonto an oder laden Sie die AWS Control Tower-Konsole neu, falls sie bereits geöffnet ist. Sie werden die Seite „Landing Zone Drift“ sehen. Wähle „Zurücksetzen“, um die Landezone zu reparieren.
5. Warte, bis der Reset-Vorgang abgeschlossen ist.

Wenn die Wiederherstellung erfolgreich ist, befindet sich das gemeinsame Konto in einem normalen Zustand und entspricht den Anforderungen.

Wenn das Konto durch die Schritte zur Problembehebung nicht wiederhergestellt wird, wenden Sie sich an. AWS Support

Um ein gemeinsames Konto mithilfe des AWS Control Tower wiederherzustellen und AWS Organizations Konsolen (manuelle Problembehebung)

1. Melden Sie sich bei der AWS Organizations Konsole unter anhttps://console.aws.amazon.com/organizations/. Sie müssen sich als IAM-Benutzer, Benutzer im IAM Identity Center oder als Rolle mit der `AWSOrganizationsFullAccess` verwalteten Richtlinie oder einer gleichwertigen Rolle anmelden.
2. Laden Sie das gemeinsame Konto zurück in die Organisation ein. Informationen zu den Anforderungen, Voraussetzungen und dem Verfahren für die Einladung eines Kontos zu AWS

Organizations einem Konto finden Sie im AWS Organizations Benutzerhandbuch unter Ein AWS Konto in Ihre Organisation einladen.

3. Melde dich bei dem geteilten Konto an, das entfernt wurde, und gehe dann zu https://console.aws.amazon.com/organizations/home #/invites, um die Einladung anzunehmen.
4. Melde dich erneut beim Verwaltungskonto an.
5. Melden Sie sich bei der AWS Control Tower-Konsole als Benutzer oder Rolle mit der `AWSControlTowerServiceRolePolicy` verwalteten Richtlinie oder einem Äquivalent sowie den Berechtigungen zur Ausführung aller AWS Control Tower-Aktionen an (Controltower: *).
6. Sie sehen die Seite „Landing Zone Drift“ mit einer Option zum Zurücksetzen der Landezone. Wähle „Zurücksetzen“, um die Landezone zu reparieren.
7. Warte, bis der Reset-Vorgang abgeschlossen ist.

Wenn die Wiederherstellung erfolgreich ist, befindet sich das gemeinsame Konto in einem normalen Zustand und entspricht den Anforderungen.

Wenn das Konto durch die Korrekturmaßnahmen nicht wiederhergestellt wird, wenden Sie sich an. AWS Support

Externe Änderungen, die automatisch aktualisiert werden

Änderungen, die Sie an den E-Mail-Adressen Ihres Kontos vornehmen, werden von AWS Control Tower automatisch aktualisiert, Account Factory aktualisiert sie jedoch nicht automatisch.

Ändern der E-Mail-Adresse eines geregelten Kontos

AWS Control Tower ruft E-Mail-Adressen ab und zeigt sie an, wie es für die Nutzung der Konsole erforderlich ist. Daher werden gemeinsam genutzte und andere Konto-E-Mail-Adressen aktualisiert und im AWS Control Tower einheitlich angezeigt, nachdem Sie sie geändert haben.

> **Note**
>
> In zeigt Account Factory die Parameter an AWS Service Catalog, die in der Konsole angegeben wurden, als Sie ein bereitgestelltes Produkt erstellt haben. Die ursprüngliche E-Mail-Adresse des Kontos wird jedoch nicht automatisch aktualisiert, wenn sich die E-Mail-Adresse des Kontos ändert. Dies liegt daran, dass das Konto konzeptionell innerhalb des bereitgestellten Produkts enthalten ist; es ist nicht dasselbe wie das bereitgestellte Produkt.

Um diesen Wert zu aktualisieren, müssen Sie das bereitgestellte Produkt aktualisieren, was zu einer Änderung der Governance-Position führen kann.

Anwendung externer Regeln AWS Config

AWS Control Tower zeigt den Konformitätsstatus aller AWS Config Regeln an, die in bei AWS Control Tower registrierten Organisationseinheiten implementiert wurden, einschließlich Regeln, die außerhalb der AWS Control Tower-Konsole aktiviert wurden.

Löschen von AWS Control Tower-Ressourcen außerhalb von AWS Control Tower

Sie können OUs und Konten im AWS Control Tower löschen und müssen keine weiteren Maßnahmen ergreifen, um die Updates zu sehen. Account Factory wird automatisch aktualisiert, wenn Sie eine OU löschen, aber nicht, wenn Sie ein Konto löschen.

Löschen einer registrierten OU (außer der Security OU)

Innerhalb AWS Organizations können Sie leere Organisationseinheiten (OUs) mithilfe der API oder der Konsole entfernen. OUs, die Konten enthalten, können nicht gelöscht werden.

AWS Control Tower erhält eine Benachrichtigung AWS Organizations , wenn eine OU gelöscht wird. Es aktualisiert die OU-Liste in der Account Factory, sodass die Liste der registrierten Organisationseinheiten konsistent bleibt.

> **Note**
>
> In wird die Account Factory aktualisiert AWS Service Catalog, um die gelöschte Organisationseinheit aus der Liste der verfügbaren Organisationseinheiten zu entfernen, für die Sie ein Konto einrichten können.

Löschen eines angemeldeten Kontos aus einer Organisationseinheit

Wenn Sie ein registriertes Konto löschen, erhält AWS Control Tower eine Benachrichtigung und nimmt Aktualisierungen vor, sodass die Informationen konsistent bleiben.

> **Note**
>
> In AWS Service Catalog wird das von Account Factory bereitgestellte Produkt, das das verwaltete Konto darstellt, nicht aktualisiert, um das Konto zu löschen. Stattdessen wird das

bereitgestellte Produkt als `TAINTED` und in einem Fehlerzustand angezeigt. Gehen Sie zur Bereinigung zu AWS Service Catalog, wählen Sie das bereitgestellte Produkt aus und wählen Sie dann Terminate (Beenden).

Steuern Sie Organisationen und Konten mit AWS Control Tower

Alle Organisationseinheiten (OUs) und Konten, die Sie in AWS Control Tower erstellen, werden automatisch von AWS Control Tower verwaltet. Wenn Sie bereits über Organisationseinheiten und Konten verfügen, die außerhalb von AWS Control Tower erstellt wurden, können Sie diese auch in die AWS Control Tower-Governance integrieren.

Bei bestehenden AWS Organizations AWS Konten ziehen es die meisten Kunden vor, Gruppen von Konten zu registrieren, indem sie die gesamte Organisationseinheit (OU) registrieren, die die Konten enthält. Sie können Konten auch einzeln registrieren. Weitere Informationen zur Registrierung einzelner Konten finden Sie unter. Über das Registrieren vorhandener Konten

Terminologie

- Wenn Sie eine bestehende Organisation in den AWS Control Tower integrieren, wird das als Registrierung der Organisation oder als Ausweitung der Unternehmensführung auf die Organisation bezeichnet.
- Wenn Sie ein AWS Konto in den AWS Control Tower integrieren, wird dies als Registrierung des Kontos bezeichnet.

Sehen Sie sich Ihre Organisationseinheiten und Konten an

Auf der Seite AWS Control Tower Organization können Sie alle Organisationseinheiten in Ihrem einsehen AWS Organizations, einschließlich OUs, die bei AWS Control Tower registriert sind, und derjenigen, die nicht registriert sind. Sie können verschachtelte Organisationseinheiten als Teil der Hierarchie anzeigen. Eine einfache Möglichkeit, Ihre Organisationseinheiten auf der Seite „Organisation“ anzuzeigen, besteht darin, in der Dropdownliste oben rechts die Option Nur Organisationseinheiten auszuwählen.

Auf der Seite Organisation werden alle Konten in Ihrer Organisation aufgeführt, unabhängig von der Organisationseinheit oder dem Registrierungsstatus im AWS Control Tower. Eine einfache Möglichkeit, Ihre Konten auf der Organisationsseite einzusehen, besteht darin, im Drop-down-Menü oben rechts die Option Nur Konten auszuwählen. Sie können Konten innerhalb der Organisationseinheiten einzeln anzeigen, aktualisieren und registrieren, sofern die Konten die Voraussetzungen für die Registrierung erfüllen.

Wenn Sie keine Filterung auswählen, werden Ihre Konten und Organisationseinheiten auf der Seite „Organisation“ in einer Hierarchie angezeigt. Es ist ein zentraler Ort für die Überwachung und Durchführung von Maßnahmen für alle Ihre AWS Control Tower-Ressourcen. Weitere Informationen zur Organisationsseite finden Sie in der Videoanleitung.

> **Note**
>
> Wenn Sie den vertrauenswürdigen Zugriff für die Organisation aktivieren, zu der Ihre Landing Zone gehört, kann AWS Control Tower Rollen erstellen, Ressourcen verwalten und Daten für alle Konten in der Organisation lesen. Durch den vertrauenswürdigen Zugriff sind alle Konten oder Organisationseinheiten in der Organisation für AWS Control Tower verfügbar, unabhängig davon, ob sie registriert und angemeldet sind oder nicht registriert und nicht registriert.

Video-Anleitung

Dieses Video (4:01) beschreibt, wie Sie mit der Organisationsseite im AWS Control Tower arbeiten. Wählen Sie zur besseren Ansicht das Symbol in der rechten unteren Ecke des Videos, um es in voller Bildschirmgröße anzuzeigen. Es stehen Untertitel zur Verfügung.

Videoanleitung zur Arbeit mit der Organisationsseite im AWS Control Tower.

Topics

- Registrieren Sie eine bestehende Organisationseinheit bei AWS Control Tower
- Über das Registrieren vorhandener Konten
- Ein Konto an eine andere Organisation übertragen

Erweitern Sie die Unternehmensführung auf eine bestehende Organisation

Sie können einer bestehenden Organisation AWS Control Tower Governance hinzufügen, indem Sie eine Landezone (LZ) einrichten, wie im AWS Control Tower-Benutzerhandbuch unter Erste Schritte, Schritt 2 beschrieben.

Folgendes können Sie erwarten, wenn Sie Ihre AWS Control Tower-Landezone in einer bestehenden Organisation einrichten.

- Sie können eine Landezone pro AWS Organizations Organisation haben.
- AWS Control Tower verwendet das Verwaltungskonto Ihrer bestehenden AWS Organizations Organisation als Verwaltungskonto. Es ist kein neues Verwaltungskonto erforderlich.
- AWS Control Tower richtet zwei neue Konten in einer registrierten OU ein: ein Auditkonto und ein Logging-Konto.
- Die Service Limits Ihrer Organisation müssen die Erstellung dieser beiden zusätzlichen Konten ermöglichen.
- Nachdem Sie Ihre Landing Zone gestartet oder eine OU registriert haben, gelten die AWS Control Tower-Kontrollen automatisch für alle registrierten Konten in dieser OU.
- Sie können weitere bestehende AWS Konten für eine OU registrieren, die vom AWS Control Tower verwaltet wird, sodass die Kontrollen für diese Konten gelten.
- Sie können im AWS Control Tower weitere OUs hinzufügen und bestehende OUs registrieren.

Weitere Voraussetzungen für die Registrierung und Registrierung finden Sie unter Erste Schritte mit AWS Control Tower.

Im Folgenden finden Sie weitere Informationen dazu, dass die AWS Control Tower-Kontrollen nicht für Ihre Organisationseinheiten in AWS-Organisationen gelten, für die keine AWS Control Tower-Landezonen eingerichtet sind:

- Neue Konten, die außerhalb von AWS Control Tower Account Factory erstellt wurden, unterliegen nicht den Kontrollen der registrierten Organisationseinheit.
- Neue Konten, die in Organisationseinheiten erstellt wurden, die nicht bei AWS Control Tower registriert sind, sind nicht an Kontrollen gebunden, es sei denn, Sie registrieren diese Konten ausdrücklich bei AWS Control Tower. Weitere Informationen zur Anmeldung von Konten finden Sie unter Über das Registrieren vorhandener Konten.
- Zusätzliche bestehende Organisationen, bestehende Konten und alle neuen Organisationseinheiten oder Konten, die Sie außerhalb von AWS Control Tower erstellen, sind nicht an die Kontrollen von AWS Control Tower gebunden, es sei denn, Sie registrieren die OU separat oder registrieren das Konto.

Weitere Informationen zur Anwendung von AWS Control Tower auf bestehende Organisationseinheiten und Konten finden Sie unterRegistrieren Sie eine bestehende Organisationseinheit bei AWS Control Tower.

Einen Überblick über den Prozess der Einrichtung einer AWS Control Tower-Landezone in Ihrer bestehenden Organisation finden Sie im Video im nächsten Abschnitt.

> **Note**
>
> Während der Einrichtung führt der AWS Control Tower Vorabprüfungen durch, um häufig auftretende Probleme zu vermeiden. Wenn Sie jedoch derzeit die AWS Landing Zone-Lösung für verwenden AWS Organizations, erkundigen Sie sich bei Ihrem AWS Lösungsarchitekten, bevor Sie versuchen, AWS Control Tower in Ihrer Organisation zu aktivieren, um festzustellen, ob der AWS Control Tower Ihre aktuelle Landing Zone-Bereitstellung beeinträchtigen könnte. Weitere Informationen Wenn das Konto die Voraussetzungen nicht erfüllt zum Verschieben von Konten von einer Landing Zone in eine andere finden Sie auch unter.

Video: Aktiviere eine Landing Zone in einer bestehenden AWS Organizations

In diesem Video (7:48) wird beschrieben, wie eine AWS Control Tower-Landezone in bestehenden AWS Organizations Strukturen eingerichtet und aktiviert wird. Wählen Sie zur besseren Ansicht das Symbol in der rechten unteren Ecke des Videos, um es in voller Bildschirmgröße anzuzeigen. Es stehen Untertitel zur Verfügung.

Aktivieren Sie den AWS Control Tower für bestehende Organisationen

Überlegungen für IAM Identity Center und bestehende Organisationen

- Wenn AWS IAM Identity Center (IAM Identity Center) bereits eingerichtet ist, muss die Heimatregion des AWS Control Tower mit der IAM Identity Center-Region identisch sein.
- AWS Control Tower löscht keine vorhandene Konfiguration.
- Wenn IAM Identity Center bereits aktiviert ist und Sie IAM Identity Center Directory verwenden, fügt AWS Control Tower Ressourcen wie Berechtigungssätze, Gruppen usw. hinzu und fährt wie gewohnt fort.

- Wenn ein anderes Verzeichnis (extern, AD, Managed AD) eingerichtet wird, ändert AWS Control Tower die bestehende Konfiguration nicht. Weitere Details finden Sie unter Überlegungen für AWS IAM Identity Center (IAM Identity Center) -Kunden.

Zugriff auf andere AWS service

Nachdem Sie Ihre Organisation in AWS Control Tower Governance eingeführt haben, haben Sie weiterhin Zugriff auf alle AWS Services AWS Organizations, die über die AWS Organizations Konsole und die APIs verfügbar sind. Weitere Informationen finden Sie unter Zugehörige AWS-Services.

Verschachtelte Organisationseinheiten im AWS Control Tower

In diesem Kapitel sind die Erwartungen und Überlegungen aufgeführt, die Sie bei der Arbeit mit verschachtelten Organisationseinheiten in AWS Control Tower berücksichtigen sollten. In den meisten Fällen entspricht die Arbeit mit verschachtelten Organisationseinheiten der Arbeit mit einer flachen OU-Struktur. Das Register und die Re-register Funktionen funktionieren mit verschachtelten Organisationseinheiten, mit Ausnahme der geänderten Verhaltensweisen, die in diesem Kapitel beschrieben werden.

Video-Anleitung

In diesem Video (4:46) wird beschrieben, wie verschachtelte OU-Bereitstellungen im AWS Control Tower verwaltet werden. Wählen Sie zur besseren Ansicht das Symbol in der rechten unteren Ecke des Videos, um es in voller Bildschirmgröße anzuzeigen. Es stehen Untertitel zur Verfügung.

Video-Walkthrough zur Verwaltung verschachtelter OUs im AWS Control Tower.

Anleitungen zu bewährten Methoden für verschachtelte Organisationseinheiten und Ihre Landezone finden Sie im Blogbeitrag Organizing your AWS Control Tower landing zone with nested OUs.

Erweitern Sie von der flachen OU-Struktur zur verschachtelten OU-Struktur

Wenn Sie Ihre AWS Control Tower-Landingzone mit einer flachen OU-Struktur erstellt haben, können Sie sie zu einer verschachtelten OU-Struktur erweitern.

Dieser Prozess besteht aus vier Hauptschritten:

1. Erstellen Sie Ihre gewünschte verschachtelte OU-Struktur in AWS Control Tower.

2. Gehen Sie zur AWS Organizations Konsole und verwenden Sie deren Funktion zum Massenverschieben, um die Konten von der Quell-OU (flach) in die Ziel-OU (verschachtelt) zu verschieben. Gehen Sie wie folgt vor:

   a. Gehen Sie zu der Organisationseinheit, von der Sie Konten verschieben möchten.

   b. Wählen Sie alle Konten in der OU aus.

   c. Wählen Sie Verschieben.

   > **Note**
   >
   > Dieser Schritt muss in der AWS Organizations Konsole ausgeführt werden, da der AWS Control Tower keine Move-Funktion hat.

3. Gehen Sie zur verschachtelten Organisationseinheit im AWS Control Tower und registrieren Sie Re-register sie. Alle Konten in der verschachtelten Organisationseinheit werden registriert.

   - Wenn Sie die Organisationseinheit in AWS Control Tower erstellt haben, Re-register die Organisationseinheit.
   - Wenn Sie die Organisationseinheit in erstellt haben AWS Organizations, registrieren Sie die Organisationseinheit zum ersten Mal.

4. Nachdem Ihre Konten verschoben und registriert wurden, löschen Sie die leere Organisationseinheit der obersten Ebene entweder von der AWS Organizations Konsole oder von der AWS Control Tower-Konsole.

Die Registrierung verschachtelter OU wird vorab überprüft

Um die erfolgreiche Registrierung Ihrer verschachtelten Organisationseinheiten und ihrer Mitgliedskonten zu unterstützen, führt AWS Control Tower eine Reihe von Vorabprüfungen durch. Dieselben Vorabprüfungen werden bei der Registrierung einer Organisationseinheit der obersten Ebene oder einer verschachtelten Organisationseinheit durchgeführt. Weitere Informationen finden Sie unter Häufige Fehlerursachen bei der Registrierung oder erneuten Registrierung.

- Wenn alle Vorabprüfungen bestanden sind, beginnt AWS Control Tower automatisch mit der Registrierung Ihrer OU.
- Wenn eine Vorabprüfung fehlschlägt, stoppt AWS Control Tower den Registrierungsprozess und stellt Ihnen eine Liste der Punkte zur Verfügung, die behoben werden müssen, bevor Sie Ihre OU registrieren können.

Verschachtelte Organisationseinheiten und Rollen

AWS Control Tower verteilt die `AWSControlTowerExecution` Rolle auf Konten unter der Ziel-OU und auf Konten in allen OUs, die unter der Ziel-OU verschachtelt sind, auch wenn Sie nur die Ziel-OU registrieren möchten. Diese Rolle gewährt jedem Benutzer des Verwaltungskontos Administratorberechtigungen für jedes Konto, das diese Rolle besitzt. `AWSControlTowerExecution` Die Rolle kann verwendet werden, um Aktionen auszuführen, die normalerweise von den Steuerungen des AWS Control Tower nicht zugelassen würden.

Sie können diese Rolle aus Konten löschen, die nicht registriert sind und die Sie nicht registrieren möchten. Wenn Sie diese Rolle löschen, können Sie das Konto nicht bei AWS Control Tower registrieren oder die unmittelbar übergeordneten Organisationseinheiten registrieren, es sei denn, Sie stellen die Rolle für das Konto wieder her. Um die `AWSControlTowerExecution` Rolle aus einem Konto zu löschen, müssen Sie unter der `AWSControlTowerExecution` Rolle angemeldet sein, da keine anderen IAM-Prinzipale Rollen löschen dürfen, die von AWS Control Tower verwaltet werden.

Informationen zum Einschränken des Rollenzugriffs finden Sie unter Optionale Bedingungen für Ihre Rollenvertrauensbeziehungen.

Was passiert bei der Registrierung und erneuten Registrierung von verschachtelten Organisationseinheiten und Konten

Wenn Sie eine verschachtelte Organisationseinheit registrieren oder erneut registrieren, registriert AWS Control Tower alle nicht registrierten Konten der Ziel-OU und aktualisiert alle registrierten Konten. Folgendes können Sie erwarten.

AWS Control Tower führt die folgenden Aufgaben aus

- Fügt die `AWSControlTowerExecution` Rolle allen nicht registrierten Konten unter dieser Organisationseinheit und allen nicht registrierten Konten in ihren verschachtelten Organisationseinheiten hinzu.
- Registriert Mitgliedskonten, die nicht registriert sind.
- Re-enrolls Konten registrierter Mitglieder.
- Erstellt eine IAM Identity Center-Anmeldung für neu registrierte Mitgliedskonten.
- Aktualisiert bestehende registrierte Mitgliedskonten, um Ihre Änderungen an der Landezone widerzuspiegeln.
- Aktualisiert Steuerelemente, die für diese Organisationseinheit und ihre Mitgliedskonten konfiguriert sind.

Überlegungen zur Registrierung verschachtelter Organisationseinheiten

- Sie können keine Organisationseinheit unter der Kern-OU (Security OU) registrieren.
- Verschachtelte Organisationseinheiten müssen separat registriert werden.
- Sie können eine Organisationseinheit nur registrieren, wenn die übergeordnete Organisationseinheit registriert ist.
- Sie können eine Organisationseinheit nur registrieren, wenn alle Organisationseinheiten an höherer Stelle in der Struktur zu einem bestimmten Zeitpunkt erfolgreich registriert wurden (einige wurden möglicherweise gelöscht).
- Sie können eine Organisationseinheit registrieren, die sich unter einer höheren Organisationseinheit befindet, aber die Abweichung wird durch diese Aktion nicht repariert.

Einschränkungen bei verschachtelten Organisationseinheiten

- Organisationseinheiten können maximal 5 Ebenen tief unter dem Stamm verschachtelt werden.
- Verschachtelte Organisationseinheiten unter der Ziel-OU müssen separat registriert oder erneut registriert werden.
- Wenn sich die Ziel-Organisationseinheit in der Hierarchie auf Ebene 2 oder darunter befindet, d. h. wenn es sich nicht um eine Organisationseinheit der obersten Ebene handelt, werden präventive Kontrollen, die auf höheren Organisationseinheiten aktiviert sind, für diese Organisationseinheit und alle darunter liegenden Organisationseinheiten automatisch durchgesetzt.
- Fehler bei der OU-Registrierung werden nicht in der Hierarchiestruktur nach oben weitergegeben. Einzelheiten zum Status verschachtelter Organisationseinheiten finden Sie auf der OU-Detailseite der übergeordneten Organisationseinheit.
- Fehler bei der OU-Registrierung werden nicht im Hierarchiebaum nach unten weitergegeben.
- AWS Control Tower ändert Ihre VPC-Einstellungen für neue oder bestehende Konten nicht.

Verschachtelte Organisationseinheiten und Compliance

Von der AWS Control Tower-Konsole aus können Sie Organisationseinheiten und Konten, die nicht den Richtlinien entsprechen, auf der Seite Organisation einsehen, sodass Sie die Einhaltung von Vorschriften in größerem Maßstab nachvollziehen können.

Überlegungen zur Einhaltung der Vorschriften für verschachtelte Organisationseinheiten und Konten

- Die Konformität einer Organisationseinheit wird nicht anhand der Konformität der untergeordneten Organisationseinheiten bestimmt.
- Der Konformitätsstatus einer Steuerung wird für alle Organisationseinheiten berechnet, auf denen die Steuerung aktiviert ist, einschließlich verschachtelter Organisationseinheiten. Sehen Sie sich den AWS Control Tower-Compliance-Status für OUs und Konten an.
- Eine OU wird nur dann als nicht konform angezeigt, wenn sie Konten hat, die nicht konform sind, unabhängig davon, wo sich die OU in der OU-Hierarchie befindet.
- Wenn eine verschachtelte Organisationseinheit nicht konform ist, wird ihre übergeordnete Organisationseinheit nicht automatisch als nicht konform betrachtet.
- Auf der OU-Detail - oder Kontodetailseite können Sie eine Liste der Ressourcen einsehen, die nicht den Anforderungen entsprechen, die möglicherweise dazu führen, dass Ihre Organisationseinheiten oder Konten den Status „Nicht konform“ anzeigen.

Verschachtelte Organisationseinheiten und Drift

In bestimmten Situationen kann Drift die Registrierung verschachtelter Organisationseinheiten verhindern.

Erwartungen an Drift und verschachtelte Organisationseinheiten

- Sie können Steuerungen für OUs mit gedrifteten übergeordneten Organisationseinheiten aktivieren, aber nicht direkt für gedriftete OUs.
- Sie dürfen Detektivkontrollen unter einer geänderten Organisationseinheit aktivieren, sofern es sich nicht um eine geänderte Organisationseinheit der obersten Ebene handelt.
- Obligatorische Kontrollen sind nur für Organisationseinheiten der obersten Ebene aktiviert. Obligatorische Steuerelemente werden übersprungen, wenn Sie eine verschachtelte Organisationseinheit registrieren.
- Ein obligatorisches Steuerelement schützt AWS Config Ressourcen. Daher muss sich dieses Steuerelement in einem nicht gedrifteten Zustand befinden, um verschachtelte Organisationseinheiten registrieren zu können. Bei einem Drift blockiert der AWS Control Tower die Registrierung verschachtelter Organisationseinheiten.
- Wenn sich die Organisationseinheit der obersten Ebene im Drift befindet, kann es sein, dass die Steuerung, die die AWS Config Ressourcen schützt, sich verändert. In dieser Situation blockiert

der AWS Control Tower alle Aktionen, die die Erstellung oder Aktualisierung von AWS Config Ressourcen erfordern, einschließlich der Anwendung von Detektivkontrollen.

Verschachtelte Organisationseinheiten und Kontrollen

Wenn Sie ein Steuerelement in einer registrierten Organisationseinheit aktivieren, verhalten sich präventive und detektivische Kontrollen unterschiedlich. Bei verschachtelten Organisationseinheiten verhalten sich proaktive Kontrollen ähnlich wie detektivische Kontrollen.

Präventive Kontrollen

- Präventive Kontrollen werden für verschachtelte Organisationseinheiten durchgesetzt.
- Obligatorische präventive Kontrollen werden für alle Konten unter der Organisationseinheit und ihren verschachtelten Organisationseinheiten durchgesetzt.
- Präventive Kontrollen wirken sich auf alle Konten und Organisationseinheiten aus, die unter der Ziel-Organisationseinheit verschachtelt sind, auch wenn diese Konten und Organisationseinheiten nicht registriert sind.

Detektive und proaktive Kontrollen

- Verschachtelte Organisationseinheiten übernehmen nicht automatisch detektivische oder proaktive Kontrollen; diese müssen separat aktiviert werden.
- Detektive und proaktive Kontrollen werden nur für registrierte Konten in den Betriebsregionen deiner Landezone eingesetzt.

Kontrollstatus und Vererbung aktiviert

Sie können die vererbten Steuerelemente für jede Organisationseinheit auf der Seite mit den OU-Details anzeigen.

> **Tip**
>
> Sie können die Kontrollvererbung nutzen, um das SCP-Kontingent einer Organisationseinheit einzuhalten. Beispielsweise können Sie ein Steuerelement auf der obersten Ebene einer Organisationseinheitenhierarchie aktivieren, anstatt es direkt für eine verschachtelte Organisationseinheit zu aktivieren.

Vererbter Status

- Der Status Vererbt gibt an, dass das Steuerelement nur durch Vererbung aktiviert wird und nicht direkt auf die Organisationseinheit angewendet wurde.
- Der Status Aktiviert bedeutet, dass die Steuerung für diese Organisationseinheit durchgesetzt wird, unabhängig von ihrem Status in anderen Organisationseinheiten.
- Der Status Fehlgeschlagen bedeutet, dass die Steuerung in dieser Organisationseinheit nicht durchgesetzt wird, unabhängig von ihrem Status auf anderen Organisationseinheiten.

> **Note**
>
> Der Status Vererbt gibt an, dass die Steuerung auf eine Organisationseinheit angewendet wurde, die sich weiter oben in der Struktur befindet. Sie wird für diese Organisationseinheit erzwungen, sie wurde jedoch nicht direkt zu dieser Organisationseinheit hinzugefügt.

> **Wenn Ihre Landing Zone nicht die aktuelle Version ist**
>
> Jede Zeile in der Tabelle mit aktivierten Steuerelementen steht für ein aktiviertes Steuerelement in einer einzelnen Organisationseinheit.

Verschachtelte Organisationseinheiten und der Stamm

Das Stammverzeichnis ist keine Organisationseinheit und kann nicht registriert oder erneut registriert werden. Sie können auch keine Konten direkt im Stammverzeichnis erstellen. Das Stammverzeichnis darf nicht den Richtlinien entsprechen oder einen Lebenszyklusstatus aufweisen, z. B. registriert oder in Bearbeitung.

Das Stammverzeichnis ist jedoch der Container der obersten Ebene für alle Konten und Organisationseinheiten. Im Kontext verschachtelter Organisationseinheiten ist dies der Knoten, unter dem alle anderen Organisationseinheiten verschachtelt sind.

Registrieren Sie eine bestehende Organisationseinheit bei AWS Control Tower

Eine effiziente Möglichkeit, mehrere bestehende AWS Konten in den AWS Control Tower zu integrieren, besteht darin, die Verwaltung durch AWS Control Tower auf eine gesamte Organisationseinheit (OU) auszudehnen.

Um die AWS Control Tower-Governance für eine bestehende OU, die mit erstellt wurde AWS Organizations, und deren Konten zu aktivieren, registrieren Sie die OU in Ihrer AWS Control Tower-Landing Zone. Sie können OUs registrieren, die bis zu 1000 Konten enthalten. Wenn eine OU mehr als 1000 Konten enthält, können Sie sie nicht im AWS Control Tower registrieren.

Wenn Sie eine OU registrieren, werden ihre Mitgliedskonten in der AWS Control Tower-Landing Zone registriert. Sie unterliegen den Kontrollen, die für ihre OU gelten.

Ab Landing Zone Version 4.0 können Sie Steuerelemente direkt in einer Organisationseinheit aktivieren. Detective Controls erfordern eine AWS Config-Aufzeichnung, die aktiviert werden kann, indem Sie die OU registrieren oder die AWS Config-Aufzeichnung auf der OU aktivieren. Die Registrierung der OU wird aktiviert`AWSControlTowerBaseline`. Die Aufzeichnung in AWS Config aktivieren wird aktiviert`ConfigBaseline`. Weitere Informationen finden Sie unter Arten von Basislinien und Das Referenzhandbuch zu AWS Control Tower Controls

> **Note**
>
> Wenn Sie noch keine AWS Control Tower-Landezone haben, richten Sie zunächst eine Landezone ein, entweder in einer neuen Organisation, die von AWS Control Tower erstellt wurde, oder in einer bestehenden AWS Organizations Organisation. Weitere Informationen zum Einrichten einer Landezone finden Sie unterErste Schritte mit AWS Control Tower.

Was passiert mit meinen Konten, wenn ich meine OU registriere?

AWS Control Tower benötigt die Erlaubnis, einen vertrauenswürdigen Zugriff zwischen AWS CloudFormation und in AWS Organizations Ihrem Namen einzurichten, damit Ihr Stack automatisch für die Konten in Ihrer Organisation bereitgestellt werden AWS CloudFormation kann.

- Die `AWSControlTowerExecution` Rolle wird allen Konten mit dem Status Nicht registriert hinzugefügt.

- Obligatorische Kontrollen sind für Ihre Organisationseinheit und alle zugehörigen Konten standardmäßig aktiviert, wenn Sie Ihre Organisationseinheit registrieren.

Teilweise Registrierung von Konten nach der Registrierung einer OU

Es ist möglich, eine OU erfolgreich zu registrieren, bei bestimmten Konten kann es jedoch vorkommen, dass die Registrierung für bestimmte Konten aufgehoben bleibt. In diesem Fall erfüllen diese Konten einige der Voraussetzungen für die Registrierung nicht. Wenn eine Kontoregistrierung im Rahmen der Registrierung einer Organisationseinheit nicht erfolgreich ist, wird auf der Kontoseite im Kontostatus die Meldung Registrierung fehlgeschlagen angezeigt. Möglicherweise sehen Sie auch Kontoinformationen auf Ihrer OU-Seite, z. B. 4 von 5, im Feld Konten.

Wenn Sie beispielsweise 4 von 5 sehen, bedeutet das, dass Ihre OU insgesamt 5 Konten hat und 4 von ihnen erfolgreich registriert wurden, aber ein Konto konnte während der Registrierung der Organisationseinheit nicht registriert werden. Sie können Re-Register OU auswählen, um Konten in die Registrierung aufzunehmen, nachdem Sie sichergestellt haben, dass die Konten die Registrierungsvoraussetzungen erfüllen.

Voraussetzungen für IAM-Benutzer für die Registrierung einer Organisationseinheit

Ihre AWS Identity and Access Management (IAM-) Identität (Benutzer oder Rolle) oder Ihre IAM Identity Center-Benutzeridentität muss im entsprechenden Account Factory-Portfolio enthalten sein, wenn Sie den Vorgang „Organisationseinheit registrieren“ ausführen, auch wenn Sie bereits über Berechtigungen verfügen. `Admin` Andernfalls schlägt die Erstellung der bereitgestellten Produkte bei der Registrierung fehl. Der Fehler tritt auf, weil sich AWS Control Tower bei der Registrierung einer Organisationseinheit auf die Anmeldeinformationen des IAM-Benutzers oder der IAM Identity Center-Benutzeridentität stützt.

Das entsprechende Portfolio wurde von AWS Control Tower erstellt und heißt AWS Control Tower Account Factory Portfolio. Navigieren Sie dazu, indem Sie Service Catalog > Account Factory > AWS Control Tower Account Factory Portfolio wählen. Wählen Sie dann die Registerkarte Gruppen, Rollen und Benutzer aus, um Ihre IAM- oder IAM Identity Center-Identität anzuzeigen. Weitere Informationen zum Gewähren von Zugriff finden Sie in der Dokumentation für. AWS Service Catalog

Eine bestehende OU registrieren

In der AWS Control Tower-Konsole auf der Seite Organisation können Sie alle Organisationseinheiten und Konten Ihrer Organisation in einer Hierarchie anzeigen, einschließlich

Organisationseinheiten, die bei AWS Control Tower registriert sind, und solcher, die nicht registriert sind.

Im Allgemeinen wurden nicht registrierte OUs in einer AWS Organizations anderen Landezone erstellt und unterliegen keiner anderen Landezone. Sie können vorhandene Organisationseinheiten registrieren, die bis zu 1000 Konten enthalten. Wenn eine OU mehr als 1000 Konten enthält, können Sie sie nicht im AWS Control Tower registrieren.

Um eine bestehende OU von der Konsole aus zu registrieren

1. Melden Sie sich bei der AWS Control Tower-Konsole unter an https://console.aws.amazon.com/controltower.
2. Wählen Sie im Navigationsmenü auf der linken Seite Organisation aus.
3. Wählen Sie auf der Seite „Organisation“ das Optionsfeld neben der Organisationseinheit aus, die Sie registrieren möchten, und wählen Sie dann im Dropdownmenü „Aktionen“ oben rechts die Option Organisationseinheit registrieren aus, oder wählen Sie alternativ den Namen der Organisationseinheit aus, damit Sie die Seite mit den OU-Details für diese Organisationseinheit anzeigen können.
4. Auf der Seite mit den OU-Details können Sie oben rechts im Dropdownmenü „Aktionen“ die Option Organisationseinheit registrieren auswählen.

Der Registrierungsvorgang dauert mindestens 10 Minuten, um die Verwaltung auf die OU auszudehnen, und bis zu 2 weitere Minuten für jedes weitere Konto.

Um eine bestehende OU mit APIs zu registrieren

Um eine bestehende OU bei den AWS Control Tower-APIs zu registrieren, können Sie die `EnableBaseline` API mit dem `AWSControlTowerBaseline` im `baselineIdentifier` Feld aufrufen. Weitere Informationen finden Sie unter Registrieren einer AWS Control Tower-OU nur mit APIs.

Ergebnisse der Registrierung einer vorhandenen OU

Nachdem Sie eine bestehende OU registriert haben, ermöglicht die `AWSControlTowerExecution` Rolle es AWS Control Tower, die Governance auf die einzelnen Konten auszudehnen. Die Richtlinien werden durchgesetzt, und Informationen über Kontoaktivitäten werden an Ihre Prüf- und Protokollierungskonten gemeldet.

Zu den weiteren Ergebnissen gehören die folgenden:

- `AWSControlTowerExecution` ermöglicht die Prüfung durch das Prüfungskonto von AWS Control Tower.
- `AWSControlTowerExecution`hilft Ihnen dabei, die Protokollierung Ihrer Organisation so zu konfigurieren, dass alle Protokolle für jedes Konto an das Protokollierungskonto gesendet werden.
- `AWSControlTowerExecution`stellt sicher, dass Ihre ausgewählten AWS Control Tower-Steuerelemente automatisch für jedes einzelne Konto in Ihren Organisationseinheiten sowie für jedes neue Konto gelten, das Sie in AWS Control Tower erstellen.

Für eine registrierte OU können Sie Compliance- und Sicherheitsberichte erstellen, die auf den Prüf- und Protokollierungsfunktionen der AWS Control Tower-Steuerelemente basieren. Ihre Sicherheits- und Compliance-Teams können überprüfen, ob alle Anforderungen erfüllt sind und keine Abweichungen bzgl. der Organisation aufgetreten sind. Weitere Informationen zu Drift finden Sie unterAbweichungen im AWS Control Tower erkennen und beheben.

> **Note**
>
> Eine ungewöhnliche Situation kann auftreten, wenn der AWS Control Tower OUs und ihre Konten anzeigt. Wenn Sie ein Konto in einer registrierten OU erstellt haben und dieses registrierte Konto anschließend in eine andere OU verschieben, die nicht registriert ist, insbesondere wenn Sie das Konto AWS Organizations zum Verschieben verwenden, wird auf Ihrer OU-Detailseite das Ergebnis „1 von 0“ -Konten angezeigt. Darüber hinaus haben Sie möglicherweise in dieser nicht registrierten OU ein weiteres Konto erstellt, das nicht registriert ist. Wenn es ein unregistriertes Konto gibt, wird auf der Konsole möglicherweise „1 von 1“ für die OU angezeigt. Es sieht so aus, als ob das einzelne (neu erstellte) Konto registriert ist, aber in Wirklichkeit ist es das nicht. Sie müssen das neue Konto registrieren.

Erstellen Sie eine neue OU

So erstellen Sie eine Organisationseinheit oder eine verschachtelte Organisationseinheit in AWS Control Tower.

Um eine neue Organisationseinheit in AWS Control Tower zu erstellen

1. Navigieren Sie zur Seite „Organisation“.
2. Wählen Sie oben rechts im Dropdownmenü Ressourcen erstellen die Option Organisationseinheit erstellen aus.

3. Geben Sie einen Namen in das Feld für den Namen der Organisationseinheit ein.
4. In der Dropdownliste „Übergeordnete Organisationseinheit“ können Sie die Hierarchie der registrierten Organisationseinheiten sehen. Wählen Sie eine übergeordnete Organisationseinheit für die neue Organisationseinheit aus, die Sie erstellen.
5. Wählen Sie Hinzufügen aus.

> **Tip**
>
> Um eine verschachtelte Organisationseinheit in weniger Schritten hinzuzufügen, wählen Sie den Namen der übergeordneten Organisationseinheit aus, der in der Tabelle auf der Seite „Organisation“ angezeigt wird, rufen Sie die OU-Seite für diese übergeordnete Organisationseinheit auf und wählen Sie dann im Dropdownmenü „Aktionen“ oben rechts die Option „Organisationseinheit hinzufügen“ aus. Die neue Organisationseinheit wird automatisch als verschachtelte Organisationseinheit unter der von Ihnen ausgewählten Organisationseinheit erstellt.

> **Note**
>
> Wenn Ihre Landezone nicht auf dem neuesten Stand ist, wird im Dropdownmenü eine einfache Liste statt einer Hierarchie angezeigt. Selbst wenn Ihre Landezone verschachtelte Organisationseinheiten enthält, werden Sie in der Dropdownliste keine L5-Organisationseinheiten sehen, da Sie unter einer L5-Organisationseinheit keine neue Organisationseinheit erstellen können. Weitere Informationen zu verschachtelten OUs im AWS Control Tower finden Sie unter. Verschachtelte Organisationseinheiten im AWS Control Tower

Eine Organisationseinheit entfernen

AWS Control Tower unterstützt separate Konsolenaktionen zum Deregistrieren einer OU und zum Löschen einer OU.

Das Löschen einer OU ist endgültig. Es kann nicht rückgängig gemacht werden.

Überlegungen

- Die Organisationseinheit muss über keine Konten verfügen, damit das Löschen und Aufheben der Registrierung erfolgreich ist.
- Alle optionalen Steuerelemente müssen aus der Organisationseinheit entfernt werden.
- Sie müssen die OU deregistrieren, bevor Sie sie löschen.
- Sie können eine OU aus dem AWS Control Tower entfernen, indem Sie sie deregistrieren, ohne sie zu löschen.

Um eine OU aus dem AWS Control Tower zu entfernen

1. Melden Sie sich bei der AWS Control Tower-Konsole unter an https://console.aws.amazon.com/controltower.
2. Navigieren Sie zur Seite „Organisation“.
3. Wählen Sie den Namen der Organisationseinheit aus, um die Seite mit den OU-Details anzuzeigen, und stellen Sie sicher, dass alle Konten aus der Organisationseinheit entfernt wurden.
4. Stellen Sie außerdem auf der Seite mit den OU-Details sicher, dass alle optionalen Steuerelemente aus der OU entfernt wurden.
5. Kehren Sie zur Seite „Organisation“ zurück und wählen Sie das Optionsfeld neben der Organisationseinheit aus.
6. Wählen Sie im Dropdownmenü Aktionen oben rechts die Option Organisationseinheit abmelden aus.
7. Hören Sie hier auf, wenn Sie die Organisationseinheit nicht vollständig löschen möchten, sondern sie nur vom AWS Control Tower abmelden möchten. Um die OU vollständig zu löschen, fahren Sie mit dem nächsten Schritt fort.
8. Um fortzufahren, wählen Sie im Dropdownmenü Aktionen oben rechts die Option Löschen aus.

Sie müssen warten, bis der Abmeldevorgang abgeschlossen ist, bevor Sie eine andere Organisationseinheit abmelden können.

> **Note**
>
> Um von AWS Control Tower verwaltete Konten zu entfernen, können Sie im linken Navigationsbereich der AWS Control Tower-Konsole zu Account Factory navigieren. Um

Konten in der OU zu entfernen, die nicht von AWS Control Tower verwaltet werden, gehen Sie zur AWS Organizations Konsole.

Um eine OU programmgesteuert zu deregistrieren, rufen Sie die API auf. `DisableBaseline`

Häufige Fehlerursachen bei der Registrierung oder erneuten Registrierung

Wenn Sie eine OU registrieren oder erneut registrieren, werden im Allgemeinen alle Konten innerhalb dieser OU bei AWS Control Tower registriert. Es ist jedoch möglich, dass einige Konten nicht registriert werden, selbst wenn die gesamte OU erfolgreich registriert wurde. In diesen Fällen müssen Sie den Fehler bei der Vorabprüfung im Zusammenhang mit dem Konto beheben und dann versuchen, das Konto oder die Organisationseinheit erneut zu registrieren.

Wenn die Registrierung (oder Neuregistrierung) einer OU oder eines ihrer Mitgliedskonten fehlschlägt, gibt AWS Control Tower Fehlermeldungen für die betroffenen Mitgliedskonten zurück. Sie können die Fehlermeldungen auf der Seite mit den OU-Details einsehen, auf der eine Tabelle die Vorprüfungen und Kontofehlermeldungen zusammenfasst. Wenn ein Vorgang zur Registrierung einer Organisationseinheit fehlschlägt, werden in der Tabelle alle Fehlermeldungen für alle Konten unter der Organisationseinheit angezeigt. Bei Bedarf können Sie die Fehlermeldungen auch auf der Seite mit den Kontodetails für jedes Konto einsehen.

Optional können Sie zur Offline-Analyse eine Datei mit einem detaillierten Bericht herunterladen, aus dem hervorgeht, welche Vorabprüfungen nicht bestanden wurden. Sie können den Download abschließen, indem Sie auf die Schaltfläche Herunterladen klicken, die oben rechts im Registrierungsbereich angezeigt wird.

In diesem Abschnitt werden die Arten von Fehlern aufgeführt, die auftreten können, wenn die Vorabprüfungen fehlschlagen, und wie Sie die Fehler korrigieren können.

Fehler in der Landing Zone

- Landezone nicht bereit

  Setze deine aktuelle Landezone zurück oder aktualisiere sie auf die neueste Version.

OU-Fehler

- Überschreitet die maximale Anzahl von SCPs

Möglicherweise haben Sie das Limit für Service Control Policies (SCPs) pro OU überschritten, oder Sie haben ein anderes Kontingent erreicht. Ein Limit von 10 SCPs pro OU gilt für alle OUs in Ihrer AWS Control Tower-Landezone. Wenn Sie mehr SCPs haben, als das Kontingent zulässt, müssen Sie die SCPs löschen oder kombinieren.

- Widersprüchliche SCPs

  Bestehende SCPs können auf die Organisationseinheit oder das Konto angewendet werden, sodass AWS Control Tower das Konto nicht registrieren kann. Überprüfen Sie die angewendeten SCPs auf Richtlinien, die das Funktionieren von AWS Control Tower verhindern könnten. Achten Sie darauf, die SCPs zu überprüfen, die von OUs übernommen wurden, die in der Hierarchie weiter oben stehen.

- Übersteigt die Stack-Set-Quote

  Das Stack-Set-Kontingent wurde möglicherweise überschritten. Wenn Sie mehr Instanzen haben, als das Kontingent zulässt, müssen Sie einige Stack-Instances löschen. Weitere Informationen finden Sie unter AWS CloudFormation Kontingente im AWS CloudFormation -Benutzerhandbuch.

- Überschreitet das Kontolimit

  AWS Control Tower begrenzt jede OU bei der Registrierung auf 1000 Konten.

Fehler beim Konto

- Pre-checks auf Konten verhindert

  Ein vorhandener SCP auf der OU verhindert, dass AWS Control Tower Vorabprüfungen Ihrer OU-Mitgliedskonten durchführt. Um diesen Fehler bei der Vorabprüfung zu beheben, aktualisieren Sie den SCP oder entfernen Sie ihn aus der OU.

- Fehler in der E-Mail-Adresse

  Die E-Mail-Adresse, die Sie für das Konto angegeben haben, entspricht nicht den Benennungsstandards. Hier ist der reguläre Ausdruck (Regex), der angibt, welche Zeichen zulässig sind: `[A-Z0-9a-z._%+-]+@[A-Za-z0-9.-]+[.]+[A-Za-z]+`

- Config-Recorder oder Lieferkanal aktiviert

  Das Konto verfügt möglicherweise über einen vorhandenen AWS Config Konfigurationsrekorder oder einen Übertragungskanal. Diese müssen AWS CLI in allen AWS Regionen, in denen das

AWS Control Tower-Verwaltungskonto über regulierte Ressourcen verfügt, gelöscht oder geändert werden, bevor Sie ein Konto registrieren können.

- STS ist deaktiviert

  AWS -Security-Token-Service (AWS STS) ist möglicherweise im Konto deaktiviert. AWS STS-Endpunkte müssen in den Konten für alle Regionen aktiviert sein, die von AWS Control Tower unterstützt werden.

- IAM Identity Center-Konflikt

  Die Heimatregion des AWS Control Tower ist nicht identisch mit der Region AWS IAM Identity Center (IAM Identity Center). Wenn das IAM Identity Center bereits eingerichtet ist, muss die AWS Control Tower-Heimatregion mit der IAM Identity Center-Region identisch sein.

- Widersprüchliches SNS-Thema

  Das Konto hat einen Themennamen für Amazon Simple Notification Service (Amazon SNS), den AWS Control Tower verwenden muss. AWS Control Tower erstellt Ressourcen (wie SNS-Themen) mit bestimmten Namen. Wenn diese Namen bereits vergeben sind, schlägt die Einrichtung von AWS Control Tower fehl. Diese Situation kann auftreten, wenn Sie ein Konto wiederverwenden, das zuvor bei AWS Control Tower registriert war.

- Gesperrtes Konto erkannt

  Dieses Konto wurde gesperrt. Es kann nicht bei AWS Control Tower registriert werden. Entfernen Sie das Konto aus dieser OU und versuchen Sie es erneut.

- IAM-Benutzer nicht im Portfolio

  Fügen Sie den AWS Identity and Access Management (IAM-) Benutzer zum Service Catalog-Portfolio hinzu, bevor Sie Ihre OU registrieren. Dieser Fehler betrifft nur das Verwaltungskonto.

- Das Konto erfüllt nicht die Voraussetzungen

  Das Konto erfüllt nicht die Voraussetzungen für die Kontoregistrierung. Beispielsweise fehlen dem Konto möglicherweise Rollen und Berechtigungen, die für die Registrierung im AWS Control Tower erforderlich sind. Anweisungen zum Hinzufügen einer Rolle finden Sie unterFügen Sie die erforderliche IAM-Rolle manuell zu einer vorhandenen hinzu AWS-Konto und registriere es.

Zur Erinnerung: AWS CloudTrail Es wird automatisch für alle Ihre AWS Konten aktiviert, wenn Sie sie im AWS Control Tower registrieren. Wenn CloudTrail es vor der Registrierung für ein Konto aktiviert

ist, kann es zu einer doppelten Abrechnung kommen, es sei denn, Sie deaktivieren es, CloudTrail bevor Sie mit dem Registrierungsvorgang beginnen.

Organisationen aktualisieren

Am schnellsten können Sie eine Organisationseinheit (OU) oder mehrere Konten innerhalb einer OU aktualisieren, indem Sie eine der folgenden Aktionen ausführen:

- Re-register wenn die Organisationseinheit aktiviert `AWSControlTowerBaseline` ist.
- Setzt aktivierte Baselines zurück oder setzt aktivierte Steuerelemente zurück, falls diese Option nicht aktiviert `AWSControlTowerBaseline` ist.

Wann sollten die Organisationseinheiten und Konten von AWS Control Tower aktualisiert werden

Wenn Sie ein Landingzone-Update durchführen, müssen Sie Ihre registrierten Konten aktualisieren, um neue Kontrollen auf diese Konten anzuwenden.

- Sie können alle Konten einer Organisationseinheit aktualisieren, indem Sie die Option Re-Register oder Reset verwenden.
- Wenn Sie mehr als eine registrierte Organisationseinheit in Ihrer landing zone haben, registrieren Sie sich erneut oder setzen Sie alle Ihre Organisationseinheiten zurück, um alle Ihre Konten zu aktualisieren.
- Um ein einzelnes Konto zu aktualisieren, können Sie es über die AWS Control Tower Tower-Konsole aktualisieren oder die Option Bereitgestelltes Produkt aktualisieren auswählen, AWS Service Catalog wenn AWSControlTowerBaseline es für das Konto aktiviert ist. Siehe Aktualisiere das Konto in der Konsole.

Aktualisieren Sie mehrere Konten in derselben Organisationseinheit

Wiederholen Sie diese Schritte für jede Organisationseinheit in Ihrer AWS Control Tower Tower-Organisation, wenn Sie alle Ihre Konten und Organisationseinheiten aktualisieren müssen.

Um mehrere Konten in einer OU mit einer Aktion zu aktualisieren

1. Melden Sie sich bei der AWS Control Tower Tower-Konsole unter an https://console.aws.amazon.com/controltower.

2. Wählen Sie im linken Navigationsmenü Organisation aus.
3. Wählen Sie auf der Seite Organisation eine beliebige Organisationseinheit aus, um die Seite mit den OU-Details anzuzeigen.
4. Wenn auf der OU aktiviert AWSControlTowerBaseline ist, wählen Sie Re-Register OU unter Aktionen aus. Wenn auf der OU nicht aktiviert AWSControlTowerBaseline ist, wählen Sie unter Aktionen zum Zurücksetzen der aktivierten Baseline die Option AWS Config Baseline zurücksetzen aus und wählen Sie im Abschnitt „Enabled Controls“ die Option Enabled Controls und Reset Control aus, um aktivierte Kontrollen zurückzusetzen.

Alternativ können Sie ein beliebiges Konto auswählen, für das der Status Update verfügbar angezeigt wird, und dann für so viele Konten wie nötig die Option Konto aktualisieren auswählen.

Was passiert bei der erneuten Registrierung

Wenn Sie eine Organisationseinheit erneut registrieren:

- Das Feld AWS Control Tower Baseline-Status gibt an, ob der `AWSControlTowerBaseline` auf das Konto angewendet wurde (Aktiviert), ob der Baseline nicht angewendet wurde (Nicht aktiviert) oder ob das Anwenden der Baseline zuvor fehlgeschlagen ist (Fehlgeschlagen).
- Wenn Sie die Organisationseinheit erneut registrieren, wird die `AWSControlTowerExecution` Rolle allen Konten mit dem Status Nicht aktiviert oder Fehlgeschlagen hinzugefügt.
- AWS Control Tower erstellt eine Single Sign-On-Anmeldung (IAM Identity Center) für diese neu registrierten Konten.
- Aktivierte Konten werden erneut bei AWS Control Tower registriert.
- Fehler bei allen präventiven Kontrollen, die auf die Organisationseinheit angewendet wurden, wurden behoben, da die SCPs auf ihre Standarddefinitionen zurückgesetzt wurden.
- Alle Konten werden aktualisiert, um die neuesten Änderungen der landing zone widerzuspiegeln.

Weitere Informationen finden Sie unter Über das Registrieren vorhandener Konten.

> **Tip**
>
> Wenn Sie eine Organisationseinheit erneut registrieren oder wenn Sie Ihre landing zone Zone-Version und mehrere Mitgliedskonten aktualisieren, wird möglicherweise eine Fehlermeldung angezeigt, in der StackSet-AWSControlTowerExecutionRoleFolgendes

erwähnt wird. Dies StackSet im Verwaltungskonto kann fehlschlagen, da die AWSControlTowerExecutionIAM-Rolle bereits in allen registrierten Mitgliedskonten vorhanden ist. Bei dieser Fehlermeldung handelt es sich um ein erwartetes Verhalten, das ignoriert werden kann.

Aktualisieren Sie ein einzelnes Konto

> **Note**
>
> Die Bereitstellung, Aktualisierung und Anpassung eines einzelnen Kontos muss auf eine Organisationseinheit (OU) abzielen, für die AWSControlTowerBaseline diese Option aktiviert ist. Wenn in einer Organisationseinheit das nicht AWSControlTowerBaseline aktiviert ist, können Sie die automatische Kontoregistrierung aktivieren oder ResetEnabledControl APIs auf ResetEnabledBaseline EnabledBaselines und EnabledControls auf dieser Organisationseinheit verwenden, um Konten zu registrieren. Einzelheiten zu finden Sie unter:. AWSControlTowerBaseline Basistypen, die auf OU-Ebene gelten

Sie können einzelne AWS Control Tower Tower-Konten in der AWS Control Tower Tower-Konsole oder in der Service Catalog-Konsole aktualisieren.

Informationen zum Aktualisieren eines einzelnen Kontos in der AWS Control Tower Tower-Konsole finden Sie unterAktualisiere das Konto in der Konsole.

Um ein einzelnes Konto zu aktualisieren in AWS Service Catalog

1. Wechseln Sie zu AWS Service Catalog.
2. Wählen Sie im linken Navigationsmenü die Option Bereitgestellte Produkte aus.
3. Wählen Sie auf der Seite Bereitgestellte Produkte das Optionsfeld neben dem bereitgestellten Produkt aus, das Sie aktualisieren möchten.
4. Wählen Sie oben rechts im Drop-down-Menü Aktionen die Option Aktualisieren aus.

Weitere Informationen zur Aktualisierung finden Sie AWS Service Catalog unter Aktualisieren Sie das bereitgestellte Produkt im Service Catalog und Aktualisieren von Produkten im Service Catalog Administrator Guide.

Ein Konto an eine andere Organisation übertragen

Sie können ein Mitgliedskonto, das bei AWS Control Tower registriert ist, auf eine andere AWS Organizations Organisation übertragen.

Voraussetzungen

- Das Konto muss bei AWS Control Tower in der Quellorganisation registriert sein. Das heißt, auf das Konto wurden Basiswerte, proaktive Kontrollen oder detektivische Kontrollen angewendet.
- Das Konto muss mindestens 4 Tage vor der Übertragung erstellt worden sein.
- Sie müssen Zugriff auf das Verwaltungskonto sowohl der Quell- als auch der Zielorganisation haben.

Schritt 1: Das Konto bei AWS Control Tower abmelden

Bevor Sie das Konto übertragen, müssen Sie alle direkt darauf angewendeten AWS Control Tower Tower-Ressourcen deaktivieren. Das Konto kann weiterhin präventive Kontrollen übernehmen.

Wenn Sie Auto Enroll verwenden

Verschieben Sie das Konto an einen der folgenden Orte:

- Die Wurzel der Organisation
- Eine nicht verwaltete Organisationseinheit
- Mit Landing Zone 4.0 oder höher, eine Organisationseinheit, für die nur präventive Kontrollen aktiviert sind

Wenn Sie Auto Enroll nicht verwenden

Die folgenden Methoden sind auch verfügbar, wenn Sie Auto Enroll verwenden.

- Wählen Sie für Konten mit der AWS Control Tower- und Backup-Baseline in der AWS Control Tower Tower-Konsole die Option Unmanage aus. Sie können das bereitgestellte Produkt auch mit dem AWS Service Catalog APIs oder der Konsole beenden.
- Deaktivieren Sie für Konten mit der AWS Config-Baseline die AWS Config-Baseline auf der OU, oder verschieben Sie das Konto in das Stammverzeichnis und verwenden Sie die `DisableBaseline` API.

Schritt 2: Übertragen Sie das Konto an die Zielorganisation

Nachdem alle AWS Control Tower Tower-Baselines und -Kontrollen, die auf das Konto angewendet wurden, außer präventiven Kontrollen, deaktiviert wurden, schließen Sie die Übertragung ab.

1. Senden Sie vom Verwaltungskonto der Zielorganisation aus eine Einladung an das Mitgliedskonto.
2. Nehmen Sie die Einladung vom Mitgliedskonto an.
3. Verschieben Sie das Konto vom Verwaltungskonto der Zielorganisation in die gewünschte Organisationseinheit.

Anweisungen zum Migrationsprozess finden Sie im AWS Organizations Benutzerhandbuch unter Migrieren von AWS Konten zu einer anderen Organisation.

Schritt 3: Registrieren Sie das Konto bei der Zielorganisation

Nachdem sich das Konto in der Zielorganisation befindet, registrieren Sie es bei AWS Control Tower.

- Wenn Auto Enroll in der AWS Control Tower-Landing landing zone aktiviert ist, die für die Zielorganisation zuständig ist, wendet AWS Control Tower automatisch Baselines und Kontrollen auf das Konto an.
- Wenn Sie Auto Enroll in der Zielorganisation nicht verwenden, registrieren Sie das Konto manuell bei AWS Control Tower. Weitere Informationen finden Sie unter Über das Registrieren vorhandener Konten.

Weitere Überlegungen

Wartezeit

Konten, die über AWS Organizations Account Factory erstellt wurden, müssen mindestens 4 Tage alt sein, bevor Sie sie übertragen oder aus einer Organisation entfernen können. Weitere Informationen finden Sie im AWS Organizations Benutzerhandbuch unter Entfernen eines Mitgliedskontos aus einer Organisation.

AWS Aggregator-Grenzwerte konfigurieren

Wenn Sie mehrere Konten übertragen, erreichen Sie möglicherweise das AWS Config-Limit für die maximale Anzahl von Konten, die pro Woche für alle Aggregatoren hinzugefügt oder gelöscht werden (1.000). Informationen zur Beantragung einer Limiterhöhung finden Sie unter

AWS Config Service Limits. Sie können auch auf landing zone Version 4.0 aktualisieren, die einen serviceverknüpften Config-Aggregator verwendet. Weitere Informationen finden Sie unter AWS Konfigurationsupdates in landing zone Version 4.0.

Zugriff auf das Mitgliedskonto

Nicht registrierte Konten haben keine `AWSControlTowerExecution` Rolle. Wenn Sie die Config- oder AWS Control Tower-Baseline deaktivieren, löscht AWS Control Tower ihre Ausführungsrolle und fügt die `OrganizationsAccountAccessRole` hinzu. Sie können diese Rolle verwenden, um eine Einladung für die Zielorganisation anzunehmen.

Wenn das Konto in der Zielorganisation registriert ist, wird die `AWSControlTowerExecution` Rolle erstellt. Diese Rolle ersetzt das neue `OrganizationsAccountAccessRole` Verwaltungskonto und vertraut dem neuen Verwaltungskonto.

AWS Service Catalog und automatische Registrierung

Die automatische Registrierung wirkt sich nicht auf Ressourcen im AWS Service Catalog aus. Alle von Account Factory bereitgestellten Produkte verbleiben im Verwaltungskonto, auch wenn die Registrierung der zugrunde liegenden Konten aufgehoben wird. Informationen zur Kündigung dieser bereitgestellten Produkte im Verwaltungskonto finden Sie unter Löschen bereitgestellter Produkte im AWS Service Catalog-Benutzerhandbuch. Alle AFC-Blueprints (Account Factory Customization) verbleiben im Konto.

Integrierte Services

AWS Control Tower ist ein Service, der auf anderen AWS Services aufbaut und Sie bei der Einrichtung einer gut durchdachten Umgebung unterstützt. Dieses Kapitel bietet einen kurzen Überblick über diese Services, einschließlich Konfigurationsinformationen über die zugrunde liegenden Services und deren Funktionsweise im AWS Control Tower.

Weitere Informationen zur Messung einer gut gestalteten Umgebung finden Sie unter dem AWS Well-Architected Tool. Lesen Sie auch den Leitfaden zur Verwaltung und Verwaltung der Cloud-Umgebung.

Themen

- AWS Verfügbare Backup-Optionen
- Stellen Sie Umgebungen bereit mit CloudFormation
- Überwachen Sie Ereignisse mit CloudTrail
- Überwachen Sie Ressourcen und Dienste mit CloudWatch
- Steuern Sie Ressourcenkonfigurationen mit AWS Config
- Berechtigungen für Entitäten mit IAM verwalten
- AWS Key Management Service
- Führen Sie serverlose Rechenfunktionen mit Lambda aus
- Konten verwalten über AWS Organizations
- Speichern Sie Objekte mit Amazon S3
- Überwachen Sie Ihre Umgebung mit Security Hub CSPM
- Stellen Sie Konten bereit über AWS Service Catalog
- Verfolgen Sie Warnmeldungen über den Amazon Simple Notification Service
- Erstellen Sie verteilte Anwendungen mit AWS Step Functions

AWS Verfügbare Backup-Optionen

AWS Mit Backup können Sie einen Backup-Plan für Ihre AWS Control Tower-Landezone erstellen. Sie können einen Workflow zur Datensicherung und -wiederherstellung direkt in Ihre Landezone integrieren. Der Backup-Plan beinhaltet vordefinierte Regeln, wie z. B. Aufbewahrungstage,

Sicherungshäufigkeit und das Zeitfenster, in dem die Sicherung erfolgt. Weitere Informationen finden Sie unter AWS Backup und AWS Control Tower.

Stellen Sie Umgebungen bereit mit CloudFormation

CloudFormation ermöglicht es Ihnen, AWS Infrastrukturbereitstellungen vorhersehbar und wiederholt zu erstellen und bereitzustellen. Es hilft Ihnen, AWS Produkte zu nutzen, um äußerst zuverlässige, hoch skalierbare und kostengünstige Anwendungen in der Cloud zu erstellen, ohne sich Gedanken über die Erstellung und Konfiguration der zugrunde liegenden Infrastruktur machen zu müssen. AWS CloudFormation ermöglicht es Ihnen, eine Vorlagendatei zu verwenden, um eine Sammlung von Ressourcen zusammen als eine Einheit (einen Stapel) zu erstellen und zu löschen. Weitere Informationen finden Sie im AWS CloudFormation -Benutzerhandbuch.

AWS Control Tower verwendet CloudFormation StackSets es, um grundlegende Ressourcen wie IAM-Rollen und AWS Config -Rekorder in Ihren Konten bereitzustellen und zu verwalten. Weitere Informationen darüber, wie CloudFormation und AWS Control Tower zusammenarbeiten, finden Sie unter. Create AWS Control Tower Ressourcen mit AWS CloudFormation

Überwachen Sie Ereignisse mit CloudTrail

Der AWS Control Tower ist so konfiguriert AWS CloudTrail , dass es eine zentrale Protokollierung und Prüfung ermöglicht. Mit dieser CloudTrail Funktion kann das Verwaltungskonto Verwaltungsaktionen und Lebenszyklusereignisse für Mitgliedskonten überprüfen.

CloudTrail hilft Ihnen dabei, Ihre AWS Umgebung in der Cloud zu überwachen, indem es eine Historie der AWS API-Aufrufe für Ihre Konten führt. Sie können beispielsweise die Benutzer und Konten identifizieren, die AWS APIs für unterstützende Dienste aufgerufen haben CloudTrail, die Quell-IP-Adresse, von der aus die Aufrufe getätigt wurden, und den Zeitpunkt der Aufrufe. Sie können mithilfe der API CloudTrail in Anwendungen integrieren, die Erstellung von Trails für Ihr Unternehmen automatisieren, den Status Ihrer Trails überprüfen und steuern, wie Administratoren die CloudTrail Anmeldung ein- und ausschalten. Weitere Informationen finden Sie im AWS CloudTrail -Benutzerhandbuch.

Überwachen Sie Ressourcen und Dienste mit CloudWatch

Amazon CloudWatch bietet eine zuverlässige, skalierbare und flexible Überwachungslösung, die Sie innerhalb weniger Minuten verwenden können. Sie müssen nicht länger eigene

Überwachungssysteme und -infrastrukturen einrichten, verwalten und skalieren. Weitere Informationen finden Sie im CloudWatch Amazon-Benutzerhandbuch .

Weitere Informationen darüber, wie Amazon mit AWS Control Tower CloudWatch zusammenarbeitet, finden Sie unter Überwachung.

Steuern Sie Ressourcenkonfigurationen mit AWS Config

AWS Config bietet eine detaillierte Ansicht der mit Ihrem AWS Konto verknüpften Ressourcen, einschließlich der Art und Weise, wie sie konfiguriert sind, wie sie miteinander verknüpft sind und wie sich die Konfigurationen und ihre Beziehungen im Laufe der Zeit verändert haben. Weitere Informationen finden Sie im AWS Config -Entwicklerhandbuch.

AWS Config Ressourcen, die vom AWS Control Tower bereitgestellt werden, werden automatisch mit `aws-control-tower` einem Wert von `managed-by-control-tower` gekennzeichnet.

Weitere Informationen darüber, wie Ressourcen im AWS Control Tower AWS Config überwacht und aufgezeichnet werden und wie diese Ihnen in Rechnung gestellt werden, finden Sie unterÜberwachen Sie Ressourcenänderungen mit AWS Config.

AWS Control Tower wird AWS-Config-Regeln zur Implementierung von Detektivkontrollen verwendet. Weitere Informationen finden Sie unter Über Kontrollen in AWS Control Tower.

Integration von AWS Config in die Control Tower Landing Zone 4.0

Service-Linked Konfigurationsaggregator (SLCA)

AWS Control Tower implementiert jetzt einen Service-Linked Config Aggregator (SLCA) als Teil von Landing Zone 4.0+. Diese Änderung stellt eine erhebliche Verbesserung der Art und Weise dar, wie AWS Config-Daten in Ihrem gesamten Unternehmen aggregiert und verwaltet werden.

Die wichtigsten Änderungen

Bereitstellung eines neuen Service-Linked Config Aggregators

- Ein Service-Linked Config Aggregator wird in Ihrem angegebenen AWS Config-Integrationskonto bereitgestellt.
- Für Bestandskunden wird dies Ihr Auditkonto sein
- Für Neukunden ist dies das Konto, das im `config.accountId` Feld des Manifests angegeben ist

Delegierter Administrator

- Das AWS Config-Aggregatorkonto wird zum delegierten Administrator für AWS Config
- AWS Control Tower konfiguriert automatisch die delegierten Admin-Einstellungen
- Dies ermöglicht die zentrale Verwaltung von AWS Config in Ihrer gesamten Organisation

Migration von älteren Aggregatoren

Während des Upgrades auf Landing Zone 4.0:

- Der Organisationsaggregator im Verwaltungskonto wird entfernt.
- Der Kontoaggregator im Auditkonto wird entfernt.
- Diese werden durch den neuen serviceverknüpften Config Aggregator im AWS Config-Integrationsaggregatorkonto ersetzt.

Verbesserte Datenaggregation

Der dienstgebundene Config Aggregator bietet verbesserte Funktionen für die Config-Datenaggregation:

- Kann Daten von jedem AWS Config-Recorder in Ihrer Organisation aggregieren
- Beinhaltet Daten von Konten, die nicht von Control Tower verwaltet werden
- Bietet einen umfassenden Überblick über die Konfigurationselemente in Ihrem Unternehmen
- Unterstützt erweiterte Kontrollen des Datenumfangs

Wichtige Überlegungen

Konfiguration durch delegierte Administratoren

- AWS Control Tower verwendet das in Ihrem Manifest angegebene Konto für die AWS Config-Integration
- Dieses Konto wird automatisch als delegierter Administrator konfiguriert
- Für diese Konfiguration sind keine weiteren Maßnahmen seitens der Kunden erforderlich
- Für Bestandskunden wird Ihr bisheriges Security Roles-Integrationskonto (Audit-Konto) während des Landing Zone 4.0-Upgrades als zentrales Aggregatorkonto für AWS Config konfiguriert

Umfang der Datenaggregation

- Service-Linked Config Aggregator kann Konfigurationsdaten aus folgenden Quellen aggregieren:
  - Vom Control Tower verwaltete Konten
  - Non-Control Von Tower verwaltete Konten
  - Jedes Konto in Ihrer Organisation mit einem aktiven Config-Recorder

Zugriffskontrollen

- Der Zugriff auf aggregierte Daten wird über IAM-Richtlinien verwaltet
- Das zentrale Aggregatorkonto von AWS Config hat zentralen Zugriff auf alle aggregierten Daten
- Mitgliedskonten verwalten ihre individuellen AWS Config-Rekorder

Bewährte Methoden

Auswahl des Config Central Aggregator-Kontos

- Wählen Sie ein Konto, das sich der Sicherheits- und Compliance-Überwachung widmet
- Stellen Sie sicher, dass angemessene Zugriffskontrollen vorhanden sind
- Erwägen Sie, ein vorhandenes Prüf- oder Sicherheitskonto zu verwenden

Verwaltung der Daten

- Überprüfen Sie regelmäßig die aggregierten Konfigurationsdaten
- Implementieren Sie angemessene Aufbewahrungsrichtlinien
- Überwachen Sie den Status des AWS Config-Recorders kontoübergreifend

Auswirkungen der Migration

Beim Upgrade auf Landing Zone 4.0:

Vor der Migration

- Dokumentieren Sie vorhandene AWS Config-Regeln und Aggregatoren
- Überprüfen Sie die aktuellen AWS Config-Datenzugriffsmuster

- Planen Sie alle notwendigen Aktualisierungen der IAM-Richtlinien ein

Während der Migration

- Ältere AWS Config-Aggregatoren werden automatisch entfernt
- Service-Linked Config Aggregator wird bereitgestellt
- Der delegierte Administrator wird konfiguriert

Nach der Migration

- Stellen Sie sicher, dass der Service-Linked Config Aggregator ordnungsgemäß funktioniert
- Bestätigen Sie die Datenaggregation aus den Mitgliedskonten
- Aktualisieren Sie die Überwachungs- und Berichtstools nach Bedarf

Berechtigungen für Entitäten mit IAM verwalten

AWS Identity and Access Management (IAM) ist ein AWS Dienst zur Steuerung des Zugriffs auf andere AWS Dienste. Mit IAM können Sie Benutzer, Sicherheitsinformationen wie Zugriffsschlüssel und Berechtigungen, die die AWS Ressourcen angeben, auf die Ihre Benutzer und Anwendungen Zugriff erhalten, zentral verwalten.

Wenn Sie Ihre Landing Zone einrichten, kann eine Reihe von Gruppen AWS IAM Identity Center automatisch erstellt werden, wenn Sie IAM als Identitätsanbieter auswählen. Diese Gruppen verfügen über Berechtigungssätze, bei denen es sich um vordefinierte Berechtigungsrichtlinien von IAM handelt. Ihre Endbenutzer können IAM auch verwenden, um den Umfang der Berechtigungen für IAM-Benutzer und andere Entitäten innerhalb von Mitgliedskonten zu definieren.

AWS Identity and Access Management (IAM) vereinfacht die Verwaltung des Zugriffs auf AWS Konten und Geschäftsanwendungen. Sie können den IAM Identity Center-Zugriff und die Benutzerberechtigungen für alle Ihre AWS Konten im AWS Control Tower kontrollieren.

Weitere Informationen finden Sie im AWS IAM Identity Center -Benutzerhandbuch.

Wenn Sie in einem Unternehmen ansässig sind AWS-Region , das IAM nicht unterstützt, können Sie einen anderen Identitätsanbieter hinzuziehen, um Ihre eigenen Benutzer und Gruppen manuell einzurichten und zu verwalten.

AWS Key Management Service

AWS Key Management Service (AWS KMS) ermöglicht es Ihnen, Schlüssel zum Schutz Ihrer Daten zu erstellen und zu steuern. Mit AWS Control Tower können Sie Ihre Daten optional mit AWS KMS Verschlüsselungsschlüsseln verschlüsseln. Informationen dazu AWS KMS finden Sie im AWS KMS-Entwicklerhandbuch .

Informationen zum Einrichten von AWS KMS Schlüsseln mit AWS Control Tower finden Sie unter Optionales Konfigurieren von AWS KMS Schlüsseln.

Führen Sie serverlose Rechenfunktionen mit Lambda aus

Mit können Sie Code ausführen AWS Lambda, ohne Server bereitzustellen oder zu verwalten. Sie können Code für viele Arten von Anwendungen oder Back-End-Diensten ausführen, ohne dass zusätzlicher Verwaltungsaufwand anfällt. Wenn Sie Ihren Code hochladen, kann Lambda den Code mit hoher Verfügbarkeit ausführen und skalieren. Sie können Ihren Code so einrichten, dass er automatisch von anderen AWS Diensten ausgelöst wird, oder Sie können ihn direkt von einer beliebigen Web- oder mobilen App aus aufrufen.

Beispielsweise können bestimmte Rollen im AWS Control Tower-Prüfkonto programmgesteuert übernommen werden, sodass Sie andere Konten mithilfe von Lambda überprüfen können. Sie können auch AWS Control Tower-Lebenszyklusereignisse verwenden, um Lambda-Funktionen auszulösen.

Konten verwalten über AWS Organizations

AWS Organizations ist ein Kontoverwaltungsdienst, mit dem Sie mehrere AWS Konten in einer Organisation konsolidieren können, die Sie erstellen und zentral verwalten. Mit Organisationen können Sie Mitgliedskonten erstellen und bestehende Konten einladen, Ihrer Organisation beizutreten. Sie können diese Konten in Gruppen organisieren und für diese richtlinienbasierte Zugriffskontrollen definieren. Weitere Informationen finden Sie im AWS Organizations - Benutzerhandbuch.

In AWS Control Tower hilft Organizations dabei, die Abrechnung zentral zu verwalten, Zugriff, Compliance und Sicherheit zu kontrollieren und Ressourcen für Ihre AWS Mitgliedskonten gemeinsam zu nutzen. Konten sind in logischen Gruppen gruppiert, sogenannte Organisationseinheiten (Organizational Units, OUs). Weitere Informationen zu Organisationen finden Sie im AWS Organizations Benutzerhandbuch .

AWS Control Tower verwendet die folgenden Organisationseinheiten:

- Root — Der übergeordnete Container für alle Konten und alle anderen Organisationseinheiten in Ihrer Landing Zone.
- Sicherheit — Diese Organisationseinheit enthält das Protokollarchivkonto, das Auditkonto und die Ressourcen, deren Eigentümer sie sind.
- Sandbox — Diese OU wird erstellt, wenn Sie Ihre Landezone einrichten. Sie und andere untergeordnete OUs in Ihrer Landing Zone enthalten Ihre Mitgliedskonten. Dies sind die Konten, auf die Ihre Endbenutzer zugreifen, um an AWS Ressourcen zu arbeiten.

> **Note**
>
> Sie können Ihrer Landing Zone über die AWS Control Tower-Konsole auf der Seite Organisationseinheiten zusätzliche Organisationseinheiten hinzufügen.

Überlegungen

Auf Organisationseinheiten, die über den AWS Control Tower erstellt wurden, können Kontrollen angewendet werden. OUs, die außerhalb von AWS Control Tower erstellt wurden, können dies standardmäßig nicht. Sie können solche OUs jedoch registrieren. Sobald Sie eine OU registriert haben, können Sie Kontrollen auf sie und ihre Konten anwenden. Informationen zur Registrierung einer OU finden Sie unter Registrieren einer vorhandenen Organisationseinheit bei AWS Control Tower.

Speichern Sie Objekte mit Amazon S3

Bei Amazon Simple Storage Service (Amazon S3) handelt es sich um Speicher für das Internet. Mit Amazon S3 können Sie jederzeit beliebige Mengen von Daten von überall aus im Internet speichern und aufrufen. Sie können diese Aufgaben in der einfachen und intuitiven Weboberfläche der AWS-Managementkonsole ausführen. Weitere Informationen finden Sie im Amazon Simple Storage Service-Benutzerhandbuch .

Wenn Sie Ihre Landing Zone einrichten, wird in Ihrem Log-Archiv-Konto ein Amazon S3-Bucket erstellt, der alle Logs aller Konten in Ihrer Landing Zone enthält.

Überwachen Sie Ihre Umgebung mit Security Hub CSPM

AWS Control Tower ist mithilfe des AWS Security Hub CSPM-Standards namens Service-Managed Standard: AWS Control Tower in Security Hub CSPM integriert. Weitere Informationen finden Sie unter Security Hub-Standard. https://docs.aws.amazon.com/controltower/latest/userguide/security-hub-controls.html

Stellen Sie Konten bereit über AWS Service Catalog

AWS Service Catalog ermöglicht es IT-Administratoren, Portfolios zugelassener Produkte zu erstellen, zu verwalten und an Endbenutzer zu verteilen, die dann in einem personalisierten Portal Zugriff auf die benötigten Produkte haben. Zu den typischen Produkten gehören Server, Datenbanken, Websites oder Anwendungen, die mithilfe von AWS Ressourcen bereitgestellt werden.

Sie können kontrollieren, welche Benutzer Zugriff auf bestimmte Produkte haben. Auf diese Weise können Sie die Einhaltung der Unternehmensstandards durchsetzen, Produktlebenszyklen verwalten und Benutzern helfen, Produkte sicher zu finden und auf den Markt zu bringen. Weitere Informationen finden Sie im Service Catalog-Administratorhandbuch.

In AWS Control Tower können Ihre zentralen Cloud-Administratoren und Ihre Endbenutzer mithilfe von AWS Service Catalog Produkten, sogenannten benutzerdefinierten Blueprints, benutzerdefinierte Konten in Ihrer Landing Zone einrichten. Weitere Informationen finden Sie unter Schritt 2. Erstellen Sie das AWS Service Catalog Produkt.

Sie können über die AWS Service Catalog Konsole und die APIs mit AWS Control Tower-Konten interagieren. Weitere Informationen finden Sie unter Interagieren Sie mit AWS Control Tower Tower-Konten von AWS Service Catalog.

AWS Control Tower kann auch die Service Catalog-APIs nutzen, um die Kontobereitstellung und -aktualisierung weiter zu automatisieren. Einzelheiten finden Sie im AWS Service Catalog Entwicklerhandbuch.

Verfolgen Sie Warnmeldungen über den Amazon Simple Notification Service

Amazon Simple Notification Service (Amazon SNS) ist ein Webservice, der es Anwendungen, Endbenutzern und Geräten ermöglicht, Benachrichtigungen sofort aus der Cloud zu senden

und zu empfangen. Weitere Informationen finden Sie im Amazon Simple Notification Service-Entwicklerhandbuch.

AWS Control Tower verwendet Amazon SNS, um programmatische Benachrichtigungen an die E-Mail-Adressen Ihres Verwaltungskontos und Ihres Auditkontos zu senden. Diese Warnmeldungen helfen Ihnen, eine Drift innerhalb Ihrer Landezone zu verhindern. Weitere Informationen finden Sie unter Abweichungen im AWS Control Tower erkennen und beheben.

Wir verwenden auch Amazon Simple Notification Service, um Compliance-Benachrichtigungen von zu versenden AWS Config.

> **Tip**
>
> Eine der besten Möglichkeiten, AWS Control Tower Control-Compliance-Benachrichtigungen (in Ihrem Auditkonto) zu erhalten, ist das Abonnieren von`AggregateConfigurationNotifications`. Es ist ein Service, der Ihnen hilft, die Einhaltung der Vorschriften zu überprüfen. Es liefert Ihnen echte Daten über AWS Config Regeln, die nicht eingehalten werden. AWS Config verwaltet automatisch die Liste der Konten in Ihrer OU.
> Sie müssen das Abonnement manuell per E-Mail oder einer anderen Art von Abonnement abschließen, die SNS zulässt. Die Abrechnung `arn:aws:sns:`*`homeregion`*`:`*`account`*`:aws-controltower-AggregateSecurityNotifications` führt zu Ihrem Prüfungskonto.

Erstellen Sie verteilte Anwendungen mit AWS Step Functions

AWS Step Functions macht es einfach, die Komponenten verteilter Anwendungen in Form einer Reihe von Schritten in einem visuellen Arbeitsablauf zu koordinieren. Sie können schnell Zustandsautomaten entwickeln und ausführen, um die Schritte Ihrer Anwendung zuverlässig und skalierbar auszuführen. Weitere Informationen finden Sie im AWS Step Functions Entwicklerhandbuch.

Identitäts- und Zugriffsmanagement im AWS Control Tower

Um alle Vorgänge in Ihrer Landezone durchzuführen, wie z. B. die Bereitstellung von Konten in Account Factory oder die Erstellung neuer Organisationseinheiten (OUs) in der AWS Control Tower-Konsole, entweder AWS Identity and Access Management (IAM), oder Sie AWS IAM Identity Center müssen sich authentifizieren, dass Sie ein zugelassener Benutzer sind. AWS Wenn Sie beispielsweise die AWS Control Tower-Konsole verwenden, authentifizieren Sie Ihre Identität, indem Sie Ihre AWS Anmeldeinformationen angeben, die Sie von Ihrem Administrator erhalten haben.

Nachdem Sie Ihre Identität authentifiziert haben, kontrolliert IAM Ihren Zugriff auf bestimmte Vorgänge und Ressourcen AWS mit einem definierten Satz von Berechtigungen. Wenn Sie ein Kontoadministrator sind, können Sie IAM verwenden, um den Zugriff anderer IAM-Benutzer auf die Ressourcen zu kontrollieren, die Ihrem Konto zugeordnet sind.

Themen

- Authentifizierung
- Zugriffskontrolle
- Arbeiten mit AWS IAM Identity Center und AWS Control Tower
- Überblick über die Verwaltung von Zugriffsberechtigungen für Ihre AWS Control Tower-Ressourcen
- Verhindern Sie dienstübergreifenden Identitätswechsel
- Verwenden identitätsbasierter Richtlinien (IAM-Richtlinien) für AWS Control Tower

Authentifizierung

Sie haben Zugriff auf AWS jede der folgenden Arten von Identitäten:

- AWS Konto-Root-Benutzer — Wenn Sie zum ersten Mal ein AWS Konto erstellen, beginnen Sie mit einer Identität, die vollständigen Zugriff auf alle AWS Dienste und Ressourcen im Konto hat. Diese Identität wird als AWS Konto-Root-Benutzer bezeichnet. Sie haben Zugriff auf diese Identität, wenn Sie sich mit der E-Mail-Adresse und dem Passwort anmelden, mit dem Sie das Konto erstellt haben. Wir raten ausdrücklich davon ab, den Stammbenutzer für Alltagsaufgaben zu verwenden, auch nicht für administrative Aufgaben. Halten Sie sich stattdessen an die bewährte Methode, den Root-Benutzer nur zu verwenden, um Ihren ersten IAM Identity Center-Benutzer (empfohlen) oder IAM-Benutzer zu erstellen (in den meisten Anwendungsfällen keine bewährte Methode). Anschließend legen Sie die Anmeldedaten für den Root-Benutzer an einem sicheren Ort ab und

verwenden sie nur, um einige Konto- und Service-Verwaltungsaufgaben durchzuführen. Weitere Informationen finden Sie unter Wann sollten Sie sich als Root-Benutzer anmelden.

- IAM-Benutzer — Ein IAM-Benutzer ist eine Identität in Ihrem AWS Konto, die über spezifische, benutzerdefinierte Berechtigungen verfügt. Sie können die IAM-Benutzeranmeldedaten verwenden, um sich auf sicheren AWS Webseiten wie der AWS Management Console, den AWS Diskussionsforen oder dem Support Center anzumelden. AWS AWS Best Practices empfehlen, einen IAM Identity Center-Benutzer anstelle eines IAM-Benutzers zu erstellen, da ein höheres Sicherheitsrisiko besteht, wenn Sie einen IAM-Benutzer mit langfristigen Anmeldeinformationen erstellen.

  Wenn Sie einen IAM-Benutzer für einen bestimmten Zweck erstellen müssen, können Sie zusätzlich zu den Anmeldeinformationen Zugriffsschlüssel für jeden IAM-Benutzer generieren. Sie können diese Schlüssel verwenden, wenn Sie AWS Dienste programmgesteuert aufrufen, entweder über eines der verschiedenen SDKs oder mithilfe der AWS Befehlszeilenschnittstelle (CLI). Das SDK und die CLI-Tools verwenden die Zugriffsschlüssel, um Ihre Anfrage verschlüsselt zu signieren. Wenn Sie keine AWS Tools verwenden, müssen Sie die Anfrage selbst signieren. AWS Control Tower unterstützt Signature Version 4, ein Protokoll zur Authentifizierung eingehender API-Anfragen. Weitere Informationen zur Authentifizierung von Anfragen finden Sie unter Signature Version 4-Signaturprozess in der AWS Allgemeinen Referenz.
- IAM-Rolle – Eine IAM-Rolle ist eine IAM-Identität, die Sie in Ihrem Konto mit bestimmten Berechtigungen erstellen können. Eine IAM-Rolle ähnelt einem IAM-Benutzer insofern, als sie eine AWS Identität ist und über Berechtigungsrichtlinien verfügt, die festlegen, was die Identität tun kann und was nicht. AWS Eine Rolle ist jedoch nicht einer einzigen Person zugeordnet, sondern kann von allen Personen angenommen werden, die diese Rolle benötigen. Einer Rolle sind außerdem keine standardmäßigen, langfristigen Anmeldeinformationen (Passwörter oder Zugriffsschlüssel) zugeordnet. Wenn Sie eine Rolle annehmen, erhalten Sie stattdessen temporäre Anmeldeinformationen für Ihre Rollensitzung. IAM-Rollen mit temporären Anmeldeinformationen sind in folgenden Situationen hilfreich:
  - Verbundbenutzerzugriff — Anstatt einen IAM-Benutzer zu erstellen, können Sie vorhandene Identitäten aus Directory Service Ihrem Unternehmensbenutzerverzeichnis oder einem Web-Identitätsanbieter verwenden. Diese werden als Verbundbenutzer bezeichnet. AWS weist einem Verbundbenutzer eine Rolle zu, wenn der Zugriff über einen Identitätsanbieter angefordert wird. Weitere Informationen zu Verbundbenutzern finden Sie unter Verbundbenutzer und Rollen im IAM-Leitfaden.
  - AWS Servicezugriff — Eine Servicerolle ist eine IAM-Rolle, die ein Dienst annimmt, um in Ihrem Namen Aktionen in Ihrem Konto auszuführen. Wenn Sie einige AWS Serviceumgebungen

einrichten, müssen Sie eine Rolle definieren, die der Dienst übernehmen soll. Diese Dienstrolle muss alle Berechtigungen enthalten, die für den Dienst erforderlich sind, um auf die benötigten AWS Ressourcen zuzugreifen. Servicerollen unterscheiden sich von Service zu Service, aber viele erlauben Ihnen, Ihre Berechtigungen auszuwählen, solange Sie die dokumentierten Anforderungen für diesen Service erfüllen. Service-Rollen bieten nur Zugriff innerhalb Ihres Kontos und können nicht genutzt werden, um Zugriff auf Services in anderen Konten zu erteilen. Sie können eine Servicerolle in IAM erstellen, ändern und löschen. Sie können beispielsweise eine Rolle erstellen, mit der Amazon Redshift in Ihrem Namen auf einen Amazon S3-Bucket zugreifen und die im Bucket gespeicherten Daten in einen Amazon Redshift-Cluster laden kann. Weitere Informationen finden Sie im IAM-Benutzerhandbuch unter Erstellen einer Rolle zum Delegieren von Berechtigungen an einen AWS Dienst.

- Anwendungen, die auf Amazon EC2 ausgeführt werden — Sie können eine IAM-Rolle verwenden, um temporäre Anmeldeinformationen für Anwendungen zu verwalten, die auf einer Amazon EC2-Instance ausgeführt werden und CLI- oder API-Anforderungen stellen AWS . AWS Dies ist dem Speichern von Zugriffsschlüsseln in der Amazon EC2-Instance vorzuziehen. Um einer Amazon EC2-Instance eine AWS Rolle zuzuweisen und sie für alle ihre Anwendungen verfügbar zu machen, erstellen Sie ein Instance-Profil, das an die Instance angehängt wird. Ein Instance-Profil enthält die Rolle und ermöglicht Programmen, die auf der Amazon-EC2-Instance ausgeführt werden, temporäre Anmeldeinformationen zu erhalten. Weitere Informationen finden Sie unter Verwenden einer IAM-Rolle zum Erteilen von Berechtigungen für Anwendungen, die auf Amazon EC2-Instances ausgeführt werden im IAM-Benutzerhandbuch.

- Die IAM Identity Center-Benutzerauthentifizierung im IAM Identity Center-Benutzerportal wird durch das Verzeichnis gesteuert, das Sie mit IAM Identity Center verbunden haben. Die Autorisierung der AWS Konten, die Endbenutzern über das Benutzerportal zur Verfügung stehen, wird jedoch von zwei Faktoren bestimmt:
  - Wem wurde der Zugriff auf diese AWS Konten in der AWS IAM Identity Center-Konsole zugewiesen. Weitere Informationen finden Sie unter Single Sign-On Access im AWS IAM Identity Center Benutzerhandbuch.
  - Welche Berechtigungen wurden den Endbenutzern in der AWS IAM Identity Center-Konsole gewährt, um ihnen den entsprechenden Zugriff auf diese AWS Konten zu ermöglichen. Weitere Informationen finden Sie im AWS IAM Identity Center Benutzerhandbuch unter Berechtigungssätze.

Zugriffskontrolle

Um AWS Control Tower-Ressourcen oder andere AWS Ressourcen in Ihrer Landing Zone zu erstellen, zu aktualisieren, zu löschen oder aufzulisten, benötigen Sie Berechtigungen, um den Vorgang durchzuführen, und Sie benötigen Berechtigungen, um auf die entsprechenden Ressourcen zuzugreifen. Darüber hinaus benötigen Sie gültige Zugriffsschlüssel, um die Operation programmgesteuert ausführen zu können.

In den folgenden Abschnitten wird beschrieben, wie Sie die Berechtigungen für den AWS Control Tower verwalten:

Topics

- Überblick über die Verwaltung von Zugriffsberechtigungen für Ihre AWS Control Tower-Ressourcen
- Verwenden identitätsbasierter Richtlinien (IAM-Richtlinien) für AWS Control Tower

Arbeiten mit AWS IAM Identity Center und AWS Control Tower

In AWS Control Tower ermöglicht IAM Identity Center zentralen Cloud-Administratoren und Endbenutzern, den Zugriff auf mehrere AWS Konten und Geschäftsanwendungen zu verwalten. Standardmäßig verwendet AWS Control Tower diesen Service, um den Zugriff auf die über Account Factory erstellten Konten einzurichten und zu verwalten, es sei denn, Sie haben die Option ausgewählt, Ihre Identität und Zugriffskontrolle selbst zu verwalten.

Weitere Informationen zur Auswahl eines Identitätsanbieters finden Sie unterAnleitung zum IAM Identity Center.

Ein kurzes Tutorial zur Einrichtung Ihrer IAM Identity Center-Benutzer und -Berechtigungen in AWS Control Tower finden Sie in diesem Video (6:23). Wählen Sie zur besseren Ansicht das Symbol in der rechten unteren Ecke des Videos, um es in voller Bildschirmgröße anzuzeigen. Es stehen Untertitel zur Verfügung.

Videoanleitung zur Einrichtung des AWS IAM Identity Center in AWS Control Tower.

Über die Einrichtung von AWS Control Tower mit IAM Identity Center

Bei der ersten Einrichtung von AWS Control Tower können nur der Root-Benutzer und alle IAM-Benutzer mit den richtigen Berechtigungen IAM Identity Center-Benutzer hinzufügen. Nachdem

Endbenutzer der AWSAccountFactoryGruppe hinzugefügt wurden, können sie jedoch über den Account Factory Factory-Assistenten neue IAM Identity Center-Benutzer erstellen. Weitere Informationen finden Sie unter Bereitstellung und Verwaltung von Konten mit Account Factory.

Wenn Sie den empfohlenen Standard wählen, richtet AWS Control Tower Ihre landing zone mit einem vorkonfigurierten Verzeichnis ein, das Sie bei der Verwaltung von Benutzeridentitäten und Single Sign-On unterstützt, sodass Ihre Benutzer kontenübergreifend Verbundzugriff haben. Wenn Sie Ihre landing zone einrichten, wird dieses Standardverzeichnis erstellt, um Benutzergruppen und Berechtigungssätze zu enthalten.

> **Note**
>
> Sie können die Verwaltung Ihrer Organisation an ein anderes Konto als das Verwaltungskonto delegieren, indem Sie die Funktion für delegierte Administratoren von IAM Identity Center verwenden. AWS IAM Identity Center Wenn Sie sich für diese Funktion entscheiden, beachten Sie, dass Administratoren mit Zugriff auf die Verwaltung der Gruppenmitgliedschaft auch Gruppen verwalten können, die dem Verwaltungskonto zugewiesen sind. Weitere Informationen finden Sie in diesem Blogbeitrag mit dem Titel Erste Schritte mit der delegierten AWS SSO-Administration

Benutzergruppen, Rollen und Berechtigungssätze

Benutzergruppen verwalten spezielle Rollen die innerhalb ihrer freigegebenen Konten definiert sind. Rollen legen Sätze von Berechtigungen fest, die zusammengehören. Alle Mitglieder einer Gruppe erben die Berechtigungssätze oder Rollen, die der Gruppe zugeordnet sind. Sie können neue Gruppen für die Endbenutzer Ihrer Mitgliedskonten erstellen, sodass Sie benutzerdefiniert nur die Rollen zuweisen können, die für die spezifischen Aufgaben, die eine Gruppe ausführt, benötigt werden.

Die verfügbaren Berechtigungssätze decken ein breites Spektrum unterschiedlicher Benutzerberechtigungsanforderungen ab, z. B. Nur-Lese-Zugriff, AWS Control Tower Tower-Administratorzugriff und Service Catalog-Zugriff. Mit diesen Berechtigungssätzen können Ihre Endbenutzer schnell und gemäß den Richtlinien Ihres Unternehmens ihre eigenen AWS Konten in Ihrer landing zone einrichten.

Tipps zur Planung Ihrer Zuweisungen von Benutzern, Gruppen und Berechtigungen finden Sie unter Empfehlungen für die Einrichtung von Gruppen, Rollen und Richtlinien

Weitere Informationen zur Verwendung dieses Service im Kontext von AWS Control Tower finden Sie in den folgenden Themen im AWS IAM Identity Center Benutzerhandbuch.

- Weitere Informationen zum Hinzufügen von Benutzern finden Sie unter Benutzer hinzufügen.
- Weitere Informationen zum Hinzufügen von Benutzern zu Gruppen finden Sie unter Hinzufügen von Benutzern zu Gruppen.
- Weitere Informationen zum Bearbeiten von Benutzereigenschaften finden Sie unter Bearbeiten von Benutzereigenschaften.
- Informationen zum Hinzufügen einer Gruppen finden Sie unter Hinzufügen von Gruppen.

> **Warning**
>
> AWS Control Tower richtet Ihr IAM Identity Center-Verzeichnis in Ihrer Heimatregion ein. Wenn Sie Ihre landing zone in einer anderen Region einrichten und dann zur IAM Identity Center-Konsole navigieren, müssen Sie die Region in Ihre Heimatregion ändern. Löschen Sie Ihre IAM Identity Center-Konfiguration in Ihrer Heimatregion nicht.

Wissenswertes über IAM Identity Center-Konten und AWS Control Tower

Hier sind einige wichtige Dinge, die Sie bei der Arbeit mit IAM Identity Center-Benutzerkonten in AWS Control Tower wissen sollten.

- Wenn Ihr AWS IAM Identity Center-Benutzerkonto deaktiviert ist, erhalten Sie eine Fehlermeldung, wenn Sie versuchen, neue Konten in Account Factory bereitzustellen. Sie können Ihren IAM Identity Center-Benutzer in der IAM Identity Center-Konsole wieder aktivieren.
- Wenn Sie bei der Aktualisierung des bereitgestellten Produkts, das einem von Account Factory bereitgestellten Konto zugeordnet ist, eine neue IAM Identity Center-Benutzer-E-Mail-Adresse angeben, erstellt AWS Control Tower ein neues IAM Identity Center-Benutzerkonto. Das zuvor erstellte Benutzerkonto wird nicht entfernt. Wenn Sie es vorziehen, die E-Mail-Adresse des vorherigen IAM Identity Center-Benutzers aus dem IAM Identity Center zu entfernen, finden Sie AWS weitere Informationen unter Benutzer deaktivieren.
- AWS IAM Identity Center wurde in Azure Active Directory integriert, und Sie können Ihr vorhandenes Azure Active Directory mit AWS Control Tower verbinden.

- Weitere Informationen darüber, wie das Verhalten von AWS Control Tower mit AWS IAM Identity Center und verschiedenen Identitätsquellen interagiert, finden Sie in den Überlegungen zur Änderung Ihrer Identitätsquelle in der AWS IAM Identity Center-Dokumentation.

IAM Identity Center-Gruppen für AWS Control Tower

AWS Control Tower bietet vorkonfigurierte Gruppen, um Benutzer zu organisieren, die bestimmte Aufgaben in Ihren Konten ausführen. Sie können Benutzer hinzufügen und sie diesen Gruppen direkt im IAM Identity Center zuweisen. Auf diese Weise werden den Benutzern in Gruppen in Ihren Konten Berechtigungssätze zugeordnet. Aktuelle Anleitungen und bewährte Methoden zur Konfiguration Ihrer Gruppen finden Sie unter Bewährte Methoden im IAM Identity Center-Benutzerhandbuch.

Die folgenden Gruppen werden erstellt, wenn Sie Ihre landing zone einrichten.

AWSAccountFactory

Account	Berechtigungssätze	Description
Verwaltungskonto	AWSServiceCatalogEndUserAccess	Diese Gruppe wird in diesem Konto nur verwendet, um neue Konten mit Account Factory bereitzustellen.

AWSServiceCatalogAdmins

Account	Berechtigungssätze	Description
Verwaltungskonto	AWSServiceCatalogAdminFullAccess	Diese Gruppe wird in diesem Konto nur verwendet, um administrative Änderungen an Account Factory vorzunehmen. Benutzer in dieser Gruppe können keine neuen Konten einrichten, es sei denn, sie sind auch Teil der AWSAccountFactoryGruppe.

AWSControlTowerAdmins

Account	Berechtigungssätze	Description
Verwaltungskonto	AWSAdministratorAccess	Benutzer dieser Gruppe in diesem Konto sind die einzigen, die Zugriff auf die AWS Control Tower Tower-Konsole haben.
Konto protokollieren	AWSAdministratorAccess	Benutzer in diesem Konto verfügen über Administr atorzugriff.
Prüfungskonto	AWSAdministratorAccess	Benutzer in diesem Konto verfügen über Administr atorzugriff.
Mitgliedskonten	AWSOrganizationsFullAccess	Benutzer haben vollen Zugriff auf Organizations in diesem Konto.

AWSSecurityAuditPowerUsers

Account	Berechtigungssätze	Description
Verwaltungskonto	AWSPowerUserAccess	Benutzer können Aufgaben zur Anwendungsentwicklung ausführen und Ressource n und Dienste erstellen und konfigurieren, die die AWS bewusste Anwendung sentwicklung unterstützen.
Konto protokollieren	AWSPowerUserAccess	Benutzer können Aufgaben zur Anwendungsentwicklung ausführen und Ressource n und Dienste erstellen

Account	Berechtigungssätze	Description
		und konfigurieren, die die AWS bewusste Anwendung sentwicklung unterstützen.
Prüfungskonto	AWSPowerUserAccess	Benutzer können Aufgaben zur Anwendungsentwicklung ausführen und Ressource n und Dienste erstellen und konfigurieren, die die AWS bewusste Anwendung sentwicklung unterstützen.
Mitgliedskonten	AWSPowerUserAccess	Benutzer können Aufgaben zur Anwendungsentwicklung ausführen und Ressource n und Dienste erstellen und konfigurieren, die die AWS bewusste Anwendung sentwicklung unterstützen.

AWSSecurityAuditors

Account	Berechtigungssätze	Description
Verwaltungskonto	AWSReadOnlyAccess	Benutzer haben nur Lesezugri ff auf alle AWS Dienste und Ressourcen in diesem Konto.
Konto protokollieren	AWSReadOnlyAccess	Benutzer haben nur Lesezugri ff auf alle AWS Dienste und Ressourcen in diesem Konto.
Prüfungskonto	AWSReadOnlyAccess	Benutzer haben nur Lesezugri ff auf alle AWS Dienste und Ressourcen in diesem Konto.

Account	Berechtigungssätze	Description
Mitgliedskonten	AWSReadOnlyAccess	Benutzer haben nur Lesezugriff auf alle AWS Dienste und Ressourcen in diesem Konto.

AWSLogArchiveAdmins

Account	Berechtigungssätze	Description
Konto protokollieren	AWSAdministratorAccess	Benutzer in diesem Konto verfügen über Administratorzugriff.

AWSLogArchiveViewers

Account	Berechtigungssätze	Description
Konto protokollieren	AWSReadOnlyAccess	Benutzer haben nur Lesezugriff auf alle AWS Dienste und Ressourcen in diesem Konto.

AWSAuditAccountAdmins

Account	Berechtigungssätze	Description
Prüfungskonto	AWSAdministratorAccess	Benutzer in diesem Konto verfügen über Administratorzugriff.

Überblick über die Verwaltung von Zugriffsberechtigungen für Ihre AWS Control Tower-Ressourcen

Jede AWS Ressource gehört einer AWS-Konto, und die Berechtigungen zum Erstellen einer Ressource oder zum Erlangen des Zugriffs auf eine Ressource werden durch

Berechtigungsrichtlinien geregelt. Ein Kontoadministrator kann Berechtigungsrichtlinien an IAM-Identitäten (Benutzer, Gruppen und Rollen) anfügen. Einige Dienste (z. B. AWS Lambda) unterstützen auch das Anhängen von Berechtigungsrichtlinien an Ressourcen.

> **Note**
>
> Ein Kontoadministrator (oder Administrator) ist ein Benutzer mit Administratorrechten. Weitere Informationen finden Sie unter Bewährte Methoden für IAM im IAM-Benutzerhandbuch.

Wenn Sie für die Erteilung von Berechtigungen für einen Benutzer oder eine Rolle verantwortlich sind, müssen Sie die Benutzer und Rollen, für die Berechtigungen erforderlich sind, die Ressourcen, für die jeder Benutzer und jede Rolle Berechtigungen benötigt, und die spezifischen Aktionen, die für den Betrieb dieser Ressourcen zulässig sein müssen, kennen und nachverfolgen.

Themen

- Ressourcen und Betrieb des AWS Control Tower
- Über den Besitz von Ressourcen
- Verwalte den Zugriff auf Ressourcen
- Geben Sie die Richtlinienelemente an: Aktionen, Auswirkungen und Prinzipien
- Angeben von Bedingungen in einer Richtlinie

Ressourcen und Betrieb des AWS Control Tower

Im AWS Control Tower ist die primäre Ressource eine Landezone. AWS Control Tower unterstützt auch einen zusätzlichen Ressourcentyp, nämlich Kontrollen, die manchmal auch als Leitplanken bezeichnet werden. Für AWS Control Tower können Sie Kontrollen jedoch nur im Kontext einer vorhandenen Landezone verwalten. Steuerelemente können als Unterressource bezeichnet werden.

Den Ressourcen und Unterressourcen in AWS sind eindeutige Amazon-Ressourcennamen (ARNs) zugeordnet, wie im folgenden Beispiel gezeigt.

AWS Control Tower bietet eine Reihe von API-Vorgängen für die Arbeit mit AWS Control Tower-Ressourcen. Eine Liste der verfügbaren Operationen finden Sie unter AWS Control Tower, der AWS Control Tower API-Referenz.

Weitere Informationen zu den CloudFormation Ressourcen in AWS Control Tower finden Sie im AWS CloudFormation Benutzerhandbuch.

Über den Besitz von Ressourcen

Das AWS Konto ist Eigentümer der Ressourcen, die im Konto erstellt wurden, unabhängig davon, wer die Ressourcen erstellt hat. Insbesondere ist der Ressourcenbesitzer das AWS Konto der Prinzipalentität (d. h. der AWS-Konto Root-Benutzer, ein IAM Identity Center-Benutzer, ein IAM-Benutzer oder eine IAM-Rolle), die die Anforderung zur Ressourcenerstellung authentifiziert. Die Funktionsweise wird anhand der folgenden Beispiele deutlich:

- Wenn Sie die AWS Root-Benutzeranmeldedaten Ihres AWS Kontos verwenden, um eine Landing Zone einzurichten, ist Ihr AWS Konto der Eigentümer der Ressource.
- Wenn Sie in Ihrem AWS Konto einen IAM-Benutzer erstellen und diesem Benutzer Berechtigungen zum Einrichten einer Landing Zone gewähren, kann der Benutzer eine Landing Zone einrichten, sofern sein Konto die Voraussetzungen erfüllt. Ihr AWS Konto, zu dem der Benutzer gehört, ist jedoch Eigentümer der Landingzone-Ressource.
- Wenn Sie in Ihrem AWS Konto eine IAM-Rolle mit Berechtigungen zum Einrichten einer Landing Zone erstellen, kann jeder, der diese Rolle übernehmen kann, eine Landing Zone einrichten. Ihr AWS Konto, zu dem die Rolle gehört, ist Eigentümer der Landing Zone-Ressource.

Verwalte den Zugriff auf Ressourcen

Eine Berechtigungsrichtlinie beschreibt, wer Zugriff auf welche Objekte hat. Im folgenden Abschnitt werden die verfügbaren Optionen zum Erstellen von Berechtigungsrichtlinien erläutert.

> **Note**
>
> In diesem Abschnitt wird die Verwendung von IAM im Kontext von AWS Control Tower beschrieben. Er enthält keine detaillierten Informationen über den IAM-Service. Eine umfassende IAM-Dokumentation finden Sie unter Was ist IAM? im IAM-Benutzerhandbuch. Für Informationen über die Syntax und Beschreibungen von AWS -IAM-Richtlinien lesen Sie die IAM-Richtlinienreferenz im IAM-Benutzerhandbuch.

Richtlinien, die einer IAM-Identität zugeordnet sind, werden als identitätsbasierte Richtlinien (IAM-Richtlinien) bezeichnet. An Ressourcen angehängte Richtlinien werden als ressourcenbasierte Richtlinien bezeichnet.

> **Note**
>
> AWS Control Tower unterstützt nur identitätsbasierte Richtlinien (IAM-Richtlinien).

Themen

- Über identitätsbasierte Richtlinien (IAM-Richtlinien)
- Rollen erstellen und Berechtigungen zuweisen
- Resource-based Richtlinien

Über identitätsbasierte Richtlinien (IAM-Richtlinien)

Richtlinien können IAM-Identitäten angefügt werden. Sie können z. B. Folgendes tun:

- Einem Benutzer oder einer Gruppe in Ihrem Konto eine Berechtigungsrichtlinie zuordnen — Um einem Benutzer die Berechtigung zum Erstellen einer AWS Control Tower-Ressource zu gewähren, z. B. zum Einrichten einer Landing Zone, können Sie einem Benutzer oder einer Gruppe, zu der der Benutzer gehört, eine Berechtigungsrichtlinie anhängen.
- Einer Rolle eine Berechtigungsrichtlinie zuweisen (kontoübergreifende Berechtigungen gewähren) – Sie können einer IAM-Rolle eine identitätsbasierte Berechtigungsrichtlinie zuweisen, um kontoübergreifende Berechtigungen zu erteilen. Beispielsweise kann ein Administrator für ein AWS Konto (Konto A) eine Rolle erstellen, die kontoübergreifende Berechtigungen für ein anderes AWS Konto (Konto B) gewährt, oder der Administrator kann eine Rolle erstellen, die Berechtigungen für einen anderen AWS Dienst gewährt.
  1. Der Administrator von Konto A erstellt eine IAM-Rolle und fügt der Rolle, die Berechtigungen zur Verwaltung von Ressourcen in Konto A gewährt, eine Berechtigungsrichtlinie zu.
  2. Der Konto-A-Administrator fügt der Rolle eine Vertrauensrichtlinie hinzu. Die Richtlinie identifiziert Konto B als den Principal, der die Rolle übernehmen kann.
  3. Als Principal kann der Administrator von Konto B jedem Benutzer in Konto B die Erlaubnis erteilen, die Rolle zu übernehmen. Indem Benutzer in Konto B die Rolle übernehmen, können sie Ressourcen in Konto A erstellen oder darauf zugreifen.
  4. Um einem AWS Dienst die Fähigkeit (Berechtigungen) zu gewähren, die Rolle zu übernehmen, kann es sich bei dem Prinzipal, den Sie in der Vertrauensrichtlinie angeben, um einen AWS Dienst handeln.

Rollen erstellen und Berechtigungen zuweisen

Rollen und Berechtigungen ermöglichen Ihnen den Zugriff auf Ressourcen im AWS Control Tower und in anderen AWS Diensten, einschließlich des programmgesteuerten Zugriffs auf Ressourcen.

Um Zugriff zu gewähren, fügen Sie Ihren Benutzern, Gruppen oder Rollen Berechtigungen hinzu:

- Benutzer und Gruppen in AWS IAM Identity Center:

  Erstellen Sie einen Berechtigungssatz. Befolgen Sie die Anweisungen unter Erstellen eines Berechtigungssatzes im AWS IAM Identity Center -Benutzerhandbuch.
- Benutzer, die in IAM über einen Identitätsanbieter verwaltet werden:

  Erstellen Sie eine Rolle für den Identitätsverbund. Befolgen Sie die Anleitung unter Eine Rolle für einen externen Identitätsanbieter (Verbund) erstellen im IAM-Benutzerhandbuch.
- IAM-Benutzer:
  - Erstellen Sie eine Rolle, die Ihr Benutzer annehmen kann. Befolgen Sie die Anleitung unter Eine Rolle für einen IAM-Benutzer erstellen im IAM-Benutzerhandbuch.
  - (Nicht empfohlen) Weisen Sie einem Benutzer eine Richtlinie direkt zu oder fügen Sie einen Benutzer zu einer Benutzergruppe hinzu. Befolgen Sie die Anweisungen unter Hinzufügen von Berechtigungen zu einem Benutzer (Konsole) im IAM-Benutzerhandbuch.

Weitere Informationen zum Delegieren von Berechtigungen mithilfe von IAM finden Sie unter Zugriffsverwaltung im IAM-Benutzerhandbuch.

> **Note**
>
> Wenn Sie eine AWS Control Tower-Landing Zone einrichten, benötigen Sie einen Benutzer oder eine Rolle mit der AdministratorAccess verwalteten Richtlinie. (arn:aws:iam: :aws:) policy/AdministratorAccess

Um eine Rolle für einen zu erstellen AWS-Service (IAM-Konsole)

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die IAM-Konsole unter. https://console.aws.amazon.com/iam/
2. Klicken Sie im Navigationsbereich der IAM-Konsole auf Rollen, und wählen Sie dann Rolle erstellen.

3. Wählen Sie für Vertrauenswürdige Entität die Option AWS-Service aus.
4. Wählen Sie unter Service oder Anwendungsfall einen Service und anschließend den Anwendungsfall aus. Anwendungsfälle werden vom Dienst so definiert, dass sie die für den Dienst erforderliche Vertrauensrichtlinie enthalten.
5. Wählen Sie Weiter aus.
6. Bei Berechtigungsrichtlinien hängen die Optionen vom ausgewählten Anwendungsfall ab:

   - Wenn der Service die Berechtigungen für die Rolle definiert, können Sie keine Berechtigungsrichtlinien auswählen.
   - Wählen Sie aus einer begrenzten Anzahl von Berechtigungsrichtlinien.
   - Wählen Sie aus allen Berechtigungsrichtlinien.
   - Wählen Sie keine Berechtigungsrichtlinien aus, erstellen Sie die Richtlinien, nachdem die Rolle erstellt wurde, und fügen Sie die Richtlinien dann der Rolle an.
7. (Optional) Legen Sie eine Berechtigungsgrenze fest. Dies ist ein erweitertes Feature, das für Servicerollen verfügbar ist, aber nicht für servicegebundene Rollen.

   a. Öffnen Sie den Abschnitt Berechtigungsgrenze festlegen und wählen Sie dann Eine Berechtigungsgrenze verwenden, um die maximalen Rollenberechtigungen zu steuern aus.

      IAM enthält eine Liste der AWS verwalteten und vom Kunden verwalteten Richtlinien in Ihrem Konto.

   b. Wählen Sie die Richtlinie aus, die für eine Berechtigungsgrenze verwendet werden soll.
8. Wählen Sie Weiter aus.
9. Für den Rollennamen hängen die Optionen vom Service ab:

   - Wenn der Name der Rolle durch den Service definiert wird, können Sie den Namen der Rolle nicht bearbeiten.
   - Wenn der Service ein Präfix für den Rollennamen definiert, können Sie ein optionales Suffix eingeben.
   - Wenn der Service den Rollennamen nicht definiert, können Sie der Rolle einen Namen geben.

   Important

   Beachten Sie beim Benennen einer Rolle Folgendes:

   - Rollennamen müssen innerhalb Ihres AWS-Konto Unternehmens eindeutig sein und dürfen nicht von Groß- und Kleinschreibung abhängig gemacht werden.

Erstellen Sie beispielsweise keine Rollen mit dem Namen **`PRODROLE`** und **`prodrole`**. Wenn ein Rollenname in einer Richtlinie oder als Teil einer ARN verwendet wird, muss die Groß-/Kleinschreibung des Rollennamens beachtet werden. Wenn ein Rollenname den Kunden jedoch in der Konsole angezeigt wird, z. B. während des Anmeldevorgangs, wird die Groß-/Kleinschreibung des Rollennamens nicht beachtet.

- Sie können den Namen der Rolle nach ihrer Erstellung nicht mehr bearbeiten, da andere Entitäten möglicherweise auf die Rolle verweisen.

10. (Optional) Geben Sie unter Beschreibung eine Beschreibung für die neue Rolle ein.
11. (Optional) Um die Anwendungsfälle und Berechtigungen für die Rolle zu bearbeiten, wählen Sie in den Abschnitten Schritt 1: Vertrauenswürdige Entitäten auswählen oder Schritt 2: Berechtigungen hinzufügen die Option Bearbeiten.
12. (Optional) Fügen Sie Tags als Schlüssel-Wert-Paare hinzu, um die Identifizierung, Organisation oder Suche nach der Rolle zu vereinfachen. Weitere Informationen zur Verwendung von Tags in IAM finden Sie unter Tags für AWS Identity and Access Management Ressourcen im IAM-Benutzerhandbuch.
13. Prüfen Sie die Rolle und klicken Sie dann auf Create Role (Rolle erstellen).

So verwenden Sie den JSON-Richtlinieneditor zum Erstellen einer Richtlinie

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die IAM-Konsole unter. https://console.aws.amazon.com/iam/
2. Wählen Sie im Navigationsbereich auf der linken Seite Policies (Richtlinien).

   Wenn Sie zum ersten Mal Policies (Richtlinien) auswählen, erscheint die Seite Welcome to Managed Policies (Willkommen bei verwalteten Richtlinien). Wählen Sie Get Started.
3. Wählen Sie oben auf der Seite Create policy (Richtlinie erstellen) aus.
4. Wählen Sie im Bereich Policy editor (Richtlinien-Editor) die Option JSON aus.
5. Geben oder fügen Sie ein JSON-Richtliniendokument ein. Weitere Informationen zur IAM-Richtliniensprache finden Sie in der IAM-JSON-Richtlinienreferenz.
6. Beheben Sie alle Sicherheitswarnungen, Fehler oder allgemeinen Warnungen, die während der Richtlinien-Validierung erzeugt wurden, und wählen Sie dann Weiter.

> **Note**
>
> Sie können jederzeit zwischen den Editoroptionen Visual und JSON wechseln. Wenn Sie jedoch Änderungen vornehmen oder im Visual-Editor Weiter wählen, strukturiert IAM Ihre Richtlinie möglicherweise um, um sie für den visuellen Editor zu optimieren. Weitere Informationen finden Sie unter Richtlinienrestrukturierung im IAM-Benutzerhandbuch.

7. (Optional) Wenn Sie eine Richtlinie in der erstellen oder bearbeiten AWS-Managementkonsole, können Sie eine JSON- oder YAML-Richtlinienvorlage generieren, die Sie in CloudFormation Vorlagen verwenden können.

   Wählen Sie dazu im Richtlinieneditor Aktionen und dann CloudFormation Vorlage generieren aus. Weitere Informationen CloudFormation dazu finden Sie in der Referenz zum AWS Identity and Access Management Ressourcentyp im AWS CloudFormation Benutzerhandbuch.
8. Wenn Sie mit dem Hinzufügen von Berechtigungen zur Richtlinie fertig sind, wählen Sie Next (Weiter) aus.
9. Geben Sie auf der Seite Prüfen und erstellen unter Richtlinienname einen Namen und unter Beschreibung (optional) eine Beschreibung für die Richtlinie ein, die Sie erstellen. Überprüfen Sie Permissions defined in this policy (In dieser Richtlinie definierte Berechtigungen), um die Berechtigungen einzusehen, die von Ihrer Richtlinie gewährt werden.
10. (Optional) Fügen Sie der Richtlinie Metadaten hinzu, indem Sie Tags als Schlüssel-Wert-Paare anfügen. Weitere Informationen zur Verwendung von Tags in IAM finden Sie unter Tags für AWS Identity and Access Management Ressourcen im IAM-Benutzerhandbuch.
11. Wählen Sie Create policy (Richtlinie erstellen) aus, um Ihre neue Richtlinie zu speichern.

So verwenden Sie den visuellen Editor zum Erstellen einer Richtlinie

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die IAM-Konsole unter https://console.aws.amazon.com/iam/.
2. Wählen Sie im Navigationsbereich auf der linken Seite Policies (Richtlinien).

   Wenn Sie zum ersten Mal Policies (Richtlinien) auswählen, erscheint die Seite Welcome to Managed Policies (Willkommen bei verwalteten Richtlinien). Wählen Sie Get Started.
3. Wählen Sie Richtlinie erstellen aus.

4. Suchen Sie im Abschnitt Richtlinien-Editor den Abschnitt Wählen Sie einen Dienst aus, und wählen Sie dann einen AWS-Service aus. Sie können das Suchfeld oben verwenden, um die Ergebnisse in der Liste der Services einzuschränken. Sie können nur einen Service innerhalb eines Berechtigungsblocks des visuellen Editors auswählen. Um mehr als einem Service Zugriff zu gewähren, fügen Sie mehrere Berechtigungsblöcke hinzu, indem Sie Add more permissions (Weitere Berechtigungen hinzufügen) auswählen.
5. Wählen Sie unter Actions allowed (Zulässige Aktionen) die Aktionen aus, die der Richtlinie hinzugefügt werden sollen. Es gibt folgende Möglichkeiten, Aktionen auszuwählen:

   - Markieren Sie das Kontrollkästchen für alle Aktionen.
   - Wählen Sie Aktionen hinzufügen, um den Namen einer bestimmten Aktion einzugeben. Sie können ein Platzhalterzeichen (*) verwenden, um mehrere Aktionen anzugeben.
   - Wählen Sie eine der Access level ((Zugriffsebene)-Gruppen aus, um alle Aktionen für die Zugriffsebene auszuwählen (z. B. Read (Lesen), Write (Schreiben) oder List (Auflisten).
   - Erweitern Sie die einzelnen Gruppen Access level (Zugriffsebene), um einzelne Aktionen auszuwählen.

   Standardmäßig lässt die Richtlinie, die Sie erstellen, die Aktionen zu, die Sie auswählen. Um die ausgewählten Aktionen stattdessen zu verweigern, wählen Sie Switch to deny permissions (Zu Berechtigungen verweigern wechseln). Da IAM standardmäßig verweigert, empfehlen wir, dass Sie im Sinne bewährter Sicherheitsmethoden nur für jene Aktionen und Ressourcen Berechtigungen zulassen, für die ein Benutzer Zugriff benötigt. Erstellen Sie eine JSON-Anweisung, um Berechtigungen nur dann zu verweigern, wenn Sie eine durch eine andere Anweisung oder Richtlinie separat zugelassene Berechtigung außer Kraft setzen möchten. Wir empfehlen, die Anzahl der Verweigerungsberechtigungen auf ein Minimum zu beschränken, da diese die Fehlerbehebung bei Berechtigungen erschweren.
6. Wenn bei Resources (Ressourcen) der Service und die Aktionen, die Sie in den vorherigen Schritten ausgewählt haben, nicht die Auswahl bestimmter Ressourcen unterstützen, sind alle Ressourcen zulässig, und Sie können diesen Abschnitt nicht bearbeiten.

   Wenn Sie eine oder mehrere Aktionen auswählen, die Berechtigungen auf Ressourcenebene unterstützen, dann listet der visuelle Editor diese Ressourcen auf. Sie können dann Resources (Ressourcen) erweitern, um die Ressourcen für Ihre Richtlinie anzugeben.

   Sie können Ressourcen auf folgende Weise angeben:

- Wählen Sie Add ARNs (ARNs hinzufügen) aus, um Ressourcen anhand ihres Amazon-Ressourcennamens (ARN) anzugeben. Sie können den visuellen ARN-Editor verwenden oder ARNs manuell auflisten. Weitere Informationen zur ARN-Syntax finden Sie unter Amazon Resource Names (ARNs) im IAM-Benutzerhandbuch. Informationen zur Verwendung von ARNs im `Resource` Element einer Richtlinie finden Sie unter IAM JSON-Richtlinienelemente: Ressource im IAM-Benutzerhandbuch.
- Wählen Sie Any in this account (Alle in diesem Konto) neben einer Ressource aus, um Berechtigungen für alle Ressourcen dieses Typs zu gewähren.
- Wählen Sie All (Alle) aus, um alle Ressourcen für den Service auszuwählen.

7. (Optional) Wählen Sie Request conditions - optional (Anfragebedingungen - (optional)) aus, um der Richtlinie, die Sie erstellen, Bedingungen hinzuzufügen. Bedingungen schränken die Auswirkungen einer JSON-Richtlinienanweisung ein. Sie können beispielsweise festlegen, dass einem Benutzer erlaubt wird, die Aktionen für die Ressourcen nur durchzuführen, wenn die Anforderung dieses Benutzers in einem bestimmten Zeitraum stattfindet. Sie können auch häufig verwendete Bedingungen verwenden, um einzuschränken, ob ein Benutzer mithilfe eines Geräts mit mehrstufiger Authentifizierung (MFA) authentifiziert werden muss. Oder Sie können festlegen, dass die Anforderung aus einem bestimmten IP-Adressbereich stammen muss. Eine Liste aller Kontextschlüssel, die Sie in einer Richtlinienbedingung verwenden können, finden Sie in der Serviceautorisierungsreferenz unter Aktionen, Ressourcen und Bedingungsschlüssel für AWS Dienste.

   Sie haben folgende Möglichkeiten, Bedingungen auszuwählen:

   - Verwenden Sie Kontrollkästchen, um allgemein verwendete Bedingungen auszuwählen.
   - Wählen Sie Add another condition (Weitere Bedingung hinzufügen) aus, um andere Bedingungen anzugeben. Wählen Sie den Bedingungsschlüssel, den Qualifier und den Operator der Bedingung aus, und geben Sie dann einen Wert ein. Um mehr als einen Wert hinzuzufügen, wählen Sie Add (Hinzufügen) aus. Sie können davon ausgehen, dass die Werte durch einen logischen `OR` Operator miteinander verbunden sind. Wählen Sie danach Add condition (Bedingung hinzufügen) aus.

   Um mehr als eine Bedingung hinzuzufügen, wählen Sie Add another condition (Weitere Bedingung hinzufügen) aus. Wiederholen Sie diesen Vorgang nach Bedarf. Jede Bedingung gilt nur für diesen einen Berechtigungsblock des visuellen Editors. Alle Bedingungen müssen wahr

sein, damit der Berechtigungsblock ausgeführt werden kann. Mit anderen Worten, gehen Sie davon aus, dass die Bedingungen durch einen logischen AND Operator verknüpft sind.

Weitere Informationen zum Condition-Element finden Sie unter IAM-JSON-Richtlinienelemente: Bedingung im IAM-Benutzerhandbuch.

8. Um mehr Berechtigungsblöcke hinzuzufügen, wählen Sie Add more permissions (Weitere Berechtigungen hinzufügen) aus. Wiederholen Sie die Schritte 2 bis 5 für jeden Block.

> **Note**
>
> Sie können jederzeit zwischen den Editoroptionen Visual und JSON wechseln. Wenn Sie jedoch Änderungen vornehmen oder im Visual-Editor Weiter wählen, strukturiert IAM Ihre Richtlinie möglicherweise um, um sie für den visuellen Editor zu optimieren. Weitere Informationen finden Sie unter Richtlinienrestrukturierung im IAM-Benutzerhandbuch.

9. (Optional) Wenn Sie eine Richtlinie in der erstellen oder bearbeiten AWS-Managementkonsole, können Sie eine JSON- oder YAML-Richtlinienvorlage generieren, die Sie in Vorlagen verwenden können. CloudFormation

   Wählen Sie dazu im Richtlinieneditor Aktionen und dann CloudFormation Vorlage generieren aus. Weitere Informationen CloudFormation dazu finden Sie in der Referenz zum AWS Identity and Access Management Ressourcentyp im AWS CloudFormation Benutzerhandbuch.

10. Wenn Sie mit dem Hinzufügen von Berechtigungen zur Richtlinie fertig sind, wählen Sie Next (Weiter) aus.
11. Geben Sie auf der Seite Prüfen und erstellen unter Richtlinienname einen Namen und unter Beschreibung (optional) eine Beschreibung für die Richtlinie ein, die Sie erstellen. Überprüfen Sie Permissions defined in this policy (In dieser Richtlinie definierte Berechtigungen), um sicherzustellen, dass Sie die beabsichtigten Berechtigungen erteilt haben.
12. (Optional) Fügen Sie der Richtlinie Metadaten hinzu, indem Sie Tags als Schlüssel-Wert-Paare anfügen. Weitere Informationen zur Verwendung von Tags in IAM finden Sie unter Tags für AWS Identity and Access Management Ressourcen im IAM-Benutzerhandbuch.
13. Wählen Sie Create policy (Richtlinie erstellen) aus, um Ihre neue Richtlinie zu speichern.

Um programmatischen Zugriff zu gewähren

Benutzer benötigen programmatischen Zugriff, wenn sie AWS außerhalb von interagieren möchten. AWS-Managementkonsole Die Art und Weise, wie programmgesteuerter Zugriff gewährt wird, hängt vom Benutzertyp ab, der zugreift. AWS

Um Benutzern programmgesteuerten Zugriff zu gewähren, wählen Sie eine der folgenden Optionen.

Welcher Benutzer benötigt programmgesteuerten Zugriff?	Bis	Von
IAM	(Empfohlen) Verwenden Sie Konsolenanmeldedaten als temporäre Anmeldeinformationen, um programmatische Anforderungen an die AWS SDKs AWS CLI oder APIs zu signieren. AWS	Befolgen Sie die Anweisungen für die Schnittstelle, die Sie verwenden möchten. • Informationen dazu finden Sie im AWS Command Line Interface Benutzerhandbuch unter Anmeldung für AWS lokale Entwicklung. AWS CLI • Informationen zu AWS SDKs finden Sie unter Anmeldung für AWS lokale Entwicklung im Referenzhandbuch für AWS SDKs und Tools.
Mitarbeiteridentität (Benutzer, die in IAM Identity Center verwaltet werden)	Verwenden Sie temporäre Anmeldeinformationen, um programmatische Anfragen an die AWS SDKs oder AWS CLI APIs zu signieren. AWS	Befolgen Sie die Anweisungen für die Schnittstelle, die Sie verwenden möchten. • Informationen dazu finden Sie AWS IAM Identity Center im AWS Command Line Interface Benutzerhandbuch unter Configuring AWS CLI to use. AWS CLI • Informationen zu AWS SDKs, Tools und AWS

Welcher Benutzer benötigt programmgesteuerten Zugriff?	Bis	Von
		APIs finden Sie unter IAM Identity Center-Authentifizierung im Referenzhandbuch für AWS SDKs und Tools.
IAM	Verwenden Sie temporäre Anmeldeinformationen, um programmatische Anfragen an die AWS SDKs oder APIs AWS CLI zu signieren. AWS	Folgen Sie den Anweisungen unter Verwenden temporärer Anmeldeinformationen mit AWS Ressourcen im IAM-Benutzerhandbuch.

Welcher Benutzer benötigt programmgesteuerten Zugriff?	Bis	Von
IAM	(Nicht empfohlen) Verwenden Sie langfristige Anmeldeinformationen, um programmatische Anfragen an die AWS CLI, AWS SDKs oder APIs zu signieren. AWS	Befolgen Sie die Anweisungen für die Schnittstelle, die Sie verwenden möchten. • Informationen dazu finden Sie im AWS CLI Benutzerhandbuch unter Authentifizierung mit IAM-Benutzeranmeldeinformationen. AWS Command Line Interface • Informationen zu AWS SDKs und Tools finden Sie unter Authentifizieren mit langfristigen Anmeldeinformationen im Referenzhandbuch für AWS SDKs und Tools. • Informationen zu AWS APIs finden Sie unter Verwalten von Zugriffsschlüsseln für IAM-Benutzer im IAM-Benutzerhandbuch.

Schützen Sie sich vor Angreifern

Weitere Informationen dazu, wie Sie sich vor Angreifern schützen können, wenn Sie anderen AWS Dienstprinzipalen Berechtigungen gewähren, finden Sie unter Optionale Bedingungen für Ihre Rollenvertrauensbeziehungen. Indem Sie Ihren Richtlinien bestimmte Bedingungen hinzufügen, können Sie dazu beitragen, einen bestimmten Angriffstyp zu verhindern, der als Confused Deputy Attack bezeichnet wird. Dieser Angriff erfolgt, wenn eine Entität eine Entität mit höheren Rechten zu einer Aktion zwingt, z. B. durch dienstübergreifenden Identitätswechsel. Allgemeine Informationen zu den Richtlinienbedingungen finden Sie auch unter. Angeben von Bedingungen in einer Richtlinie

Weitere Informationen zur Verwendung identitätsbasierter Richtlinien mit AWS Control Tower finden Sie unter. Verwenden identitätsbasierter Richtlinien (IAM-Richtlinien) für AWS Control Tower Weitere Informationen zu Benutzern, Gruppen, Rollen und Berechtigungen finden Sie im Thema Identitäten (Benutzer, Gruppen und Rollen) im IAM-Benutzerhandbuch.

Resource-based Richtlinien

Andere Services, z. B. Amazon-S3, unterstützen auch ressourcenbasierte Berechtigungsrichtlinien. Beispielsweise können Sie einem S3 Bucket eine Richtlinie zuweisen, um die Zugriffsberechtigungen für diesen Bucket zu verwalten. AWS Control Tower unterstützt keine ressourcenbasierten Richtlinien.

Geben Sie die Richtlinienelemente an: Aktionen, Auswirkungen und Prinzipien

Sie können Ihre Landing Zone über die AWS Control Tower-Konsole oder die Landing Zone-APIs einrichten und verwalten. Um Ihre Landing Zone einzurichten, müssen Sie ein IAM-Benutzer mit Administratorberechtigungen sein, wie in einer IAM-Richtlinie definiert.

Die folgenden Elemente sind die grundlegendsten, die Sie in einer Richtlinie identifizieren können:

- Ressource – In einer Richtlinie wird der Amazon-Ressourcenname (ARN) zur Identifizierung der Ressource verwendet, für die die Richtlinie gilt. Weitere Informationen finden Sie unter Ressourcen und Betrieb des AWS Control Tower.
- Aktion – Mit Aktionsschlüsselwörtern geben Sie die Ressourcenoperationen an, die Sie zulassen oder verweigern möchten. Informationen zu den Arten von Aktionen, die ausgeführt werden können, finden Sie unter Von AWS Control Tower definierte Aktionen.
- Auswirkung – Die von Ihnen festgelegte Auswirkung, wenn der Benutzer die jeweilige Aktion anfordert – entweder „allow“ (Zugriffserlaubnis) oder „deny“ (Zugriffsverweigerung). Wenn Sie den Zugriff auf eine Ressource nicht ausdrücklich gestatten ("Allow"), wird er automatisch verweigert. Sie können den Zugriff auf eine Ressource auch explizit verweigern. So können Sie sicherstellen, dass Benutzer nicht darauf zugreifen können, auch wenn der Zugriff durch eine andere Richtlinie gestattet wird.
- Principal — Bei identitätsbasierten Richtlinien (IAM-Richtlinien) ist der Benutzer, dem die Richtlinie zugeordnet ist, der implizite Prinzipal. In ressourcenbasierten Richtlinien müssen Sie den Benutzer, das Konto, den Service oder die sonstige Entität angeben, die die Berechtigungen erhalten soll (gilt nur für ressourcenbasierte Richtlinien). AWS Control Tower unterstützt keine ressourcenbasierten Richtlinien.

Weitere Informationen zur Syntax und zu Beschreibungen von IAM-Richtlinien finden Sie in der AWS -IAM-Richtlinienreferenz im IAM-Benutzerhandbuch.

Angeben von Bedingungen in einer Richtlinie

Beim Erteilen von Berechtigungen können Sie mithilfe der IAM-Richtliniensyntax die Bedingungen angeben, unter denen die Richtlinie wirksam werden soll. Beispielsweise kann festgelegt werden, dass eine Richtlinie erst ab einem bestimmten Datum gilt. Weitere Informationen zum Angeben von Bedingungen in einer Richtliniensyntax finden Sie im Thema Bedingung im IAM Benutzerhandbuch.

Um Bedingungen auszudrücken, können Sie vordefinierte Bedingungsschlüssel verwenden. Es gibt keine spezifischen Bedingungsschlüssel für AWS Control Tower. Es gibt jedoch allgemeine AWS Bedingungsschlüssel, die Sie bei Bedarf verwenden können. Eine vollständige Liste der AWS-wide-Schlüssel finden Sie im IAM-Benutzerhandbuch unter Verfügbare Schlüssel für Bedingungen.

Verhindern Sie dienstübergreifenden Identitätswechsel

Insofern AWS kann dienstübergreifender Identitätswechsel zu einem verwirrten Stellvertreter-Problem führen. Wenn ein Dienst einen anderen Dienst anruft, kommt es zu dienstübergreifendem Identitätswechsel, wenn ein Dienst einen anderen Dienst manipuliert, um seine Berechtigungen zu nutzen, um auf eine Weise auf die Ressourcen eines Kunden zu reagieren, die sonst nicht zulässig wäre. Um diesen Angriff zu verhindern, AWS stellt Tools zur Verfügung, mit denen Sie Ihre Daten schützen können, sodass nur Dienste mit legitimen Berechtigungen Zugriff auf die Ressourcen in Ihrem Konto erhalten.

Wir empfehlen, die `aws:SourceAccount` Bedingungen `aws:SourceArn` und in Ihren Richtlinien zu verwenden, um die Berechtigungen einzuschränken, die AWS Control Tower einem anderen Service für den Zugriff auf Ihre Ressourcen gewährt.

- Verwenden Sie `aws:SourceArn` diese Option, wenn Sie möchten, dass nur eine Ressource dem dienstübergreifenden Zugriff zugeordnet wird.
- Verwenden Sie diese Option, `aws:SourceAccount` wenn Sie zulassen möchten, dass jede Ressource in diesem Konto der dienstübergreifenden Nutzung zugeordnet wird.
- Wenn der `aws:SourceArn` Wert die Konto-ID nicht enthält, z. B. den ARN für einen Amazon S3-Bucket, müssen Sie beide Bedingungen verwenden, um die Berechtigungen einzuschränken.
- Wenn Sie beide Bedingungen verwenden und der `aws:SourceArn` Wert die Konto-ID enthält, müssen der `aws:SourceAccount` Wert und das Konto im `aws:SourceArn` Wert dieselbe Konto-ID aufweisen, wenn sie in derselben Richtlinienerklärung verwendet werden

Weitere Informationen und Beispiele finden Sie unter https://docs.aws.amazon.com/controltower/latest/userguide/conditions-for-role-trust.html.

Verwenden identitätsbasierter Richtlinien (IAM-Richtlinien) für AWS Control Tower

Dieses Thema enthält Beispiele für identitätsbasierte Richtlinien, die zeigen, wie ein Kontoadministrator Berechtigungsrichtlinien an IAM-Identitäten (d. h. Benutzer, Gruppen und Rollen) anhängen und so Berechtigungen für die Ausführung von Vorgängen auf AWS Control Tower-Ressourcen gewähren kann.

> **Important**
>
> Wir empfehlen Ihnen, zunächst die einführenden Themen zu lesen, in denen die grundlegenden Konzepte und Optionen erläutert werden, die Ihnen zur Verwaltung des Zugriffs auf Ihre AWS Control Tower-Ressourcen zur Verfügung stehen. Weitere Informationen finden Sie unter Überblick über die Verwaltung von Zugriffsberechtigungen für Ihre AWS Control Tower-Ressourcen.

Für die Verwendung der AWS Control Tower-Konsole sind Berechtigungen erforderlich

AWS Control Tower erstellt automatisch drei Rollen, wenn Sie eine Landezone einrichten. Alle drei Rollen sind erforderlich, um den Zugriff auf die Konsole zu ermöglichen. AWS Control Tower teilt Berechtigungen in drei Rollen auf. Dies ist eine bewährte Methode, um den Zugriff auf ein Minimum an Aktionen und Ressourcen zu beschränken.

Drei Rollen sind für den Zugang zur Landezone erforderlich

- AWS ControlTowerAdmin Rolle
- AWS ControlTowerStackSetRole
- AWSControlTowerCloudTrailRole

Wir empfehlen Ihnen, den Zugriff auf Ihre Richtlinien für die Rollenvertrauensstellung für diese Rollen einzuschränken. Weitere Informationen finden Sie unter Optionale Bedingungen für Ihre Rollenvertrauensbeziehungen.

Sehen Sie sich den Kontrollkatalog in der Konsole an

Um Kontrollinformationen in der AWS Control Tower-Konsole anzuzeigen, müssen Sie Ihren IAM-Richtlinien zusätzliche `controlcatalog` Berechtigungen hinzufügen. Diese Berechtigungen lauten wie folgt:

- `controlcatalog:GetControl`
- `controlcatalog:ListControls`
- `controlcatalog:ListControlMappings`
- `controlcatalog:ListCommonControls`

Hier ist ein Beispiel, das die aktualisierten Berechtigungen in der Richtlinie zeigt.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Action": [
                "controlcatalog:GetControl",
                "controlcatalog:ListControls",
                "controlcatalog:ListControlMappings",
                "controlcatalog:ListCommonControls"
            ],
            "Resource": [
                "*"
            ],
            "Effect": "Allow"
        }
    ]
}
```

Sie müssen diese Berechtigungen hinzufügen, da AWS Control Tower die `controlcatalog` APIs aufruft, um bestimmte Kontrollmetadaten abzurufen, sodass die AWS Control Tower-Berechtigungen nicht ausreichen.

Weitere Informationen zur Aktualisierung Ihrer Berechtigungen finden Sie unter Rollen erstellen und Berechtigungen zuweisen.

Weitere Informationen zu `controlcatalog` IAM-Aktionen finden Sie unter Aktionen, Ressourcen und Bedingungsschlüssel für Control Catalog.

> **Note**
>
> Kontrollinformationen sind über die Control Catalog-APIs verfügbar.

AWS ControlTowerAdmin Rolle

Diese Rolle bietet dem AWS Control Tower Zugriff auf die Infrastruktur, die für die Wartung der Landezone von entscheidender Bedeutung ist. Für die `AWS ControlTowerAdmin` Rolle sind eine angehängte verwaltete Richtlinie und eine Rollenvertrauensrichtlinie für die IAM-Rolle erforderlich. Eine Rollenvertrauensrichtlinie ist eine ressourcenbasierte Richtlinie, die festlegt, welche Principals die Rolle übernehmen können.

Hier ist ein Beispielausschnitt für diese Rollenvertrauensrichtlinie:

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "controltower.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Hier ist ein Beispiel für einen AWS CLI-Befehl, um diese Rolle über die CLI zu erstellen und sie in eine Datei mit dem Namen `trust.json` einzufügen:

```
aws iam create-role --role-name AWSControlTowerAdmin --path /service-role/ --assume-
role-policy-document file://trust.json
```

Für diese Rolle sind zwei IAM-Richtlinien erforderlich.

1. Eine Inline-Richtlinie, zum Beispiel:

   JSON

   ```
   {
       "Version":"2012-10-17",
       "Statement": [
           {
               "Effect": "Allow",
               "Action": "ec2:DescribeAvailabilityZones",
               "Resource": "*"
           }
       ]
   }
   ```

2. Die darauf folgende verwaltete Richtlinie, nämlich die`AWS ControlTowerServiceRolePolicy`.

AWS ControlTowerServiceRolePolicy

Dies AWS ControlTowerServiceRolePolicy ist eine AWS verwaltete Richtlinie, die Berechtigungen für die Erstellung und Verwaltung von AWS Control Tower-Ressourcen wie AWS CloudFormation Stacksets und Stack-Instances, AWS CloudTrail Protokolldateien, einen Konfigurationsaggregator für AWS Control Tower sowie AWS Organizations Konten und Organisationseinheiten (OUs) definiert, die von AWS Control Tower verwaltet werden.

Aktualisierungen dieser verwalteten Richtlinie sind in der Tabelle zusammengefasst. Verwaltete Richtlinien für AWS Control Tower

Weitere Informationen finden Sie AWS ControlTowerServiceRolePolicy im AWS Managed Policy Reference Guide.

Richtlinie zum Vertrauen in Rollen:

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "controltower.amazonaws.com"
         ]
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Die Inline-Richtlinie lautet`AWS ControlTowerAdminPolicy`:

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Action": "ec2:DescribeAvailabilityZones",
            "Resource": "*",
            "Effect": "Allow"
        }
    ]
}
```

AWS ControlTowerIdentityCenterManagementPolicy

Diese Richtlinie gewährt Berechtigungen zur Konfiguration der IAM Identity Center (IDC) - Ressourcen in den Mitgliedskonten, die bei AWS Control Tower registriert sind. Wenn Sie bei der Einrichtung (oder Aktualisierung) der Landing Zone im AWS Control Tower IAM Identity

Center als Ihren Identitätsanbieter auswählen, wird diese Richtlinie an die Rolle angehängt. `AWSControlTowerAdmin`

Weitere Einzelheiten zu dieser Richtlinie, einschließlich der neuesten Version des JSON-Richtliniendokuments, finden Sie unter AWS ControlTowerIdentityCenterManagementPolicy im AWS Referenzhandbuch für verwaltete Richtlinien.

AWS ControlTowerStackSetRole

CloudFormation übernimmt diese Rolle, um Stack-Sets in Konten bereitzustellen, die von AWS Control Tower erstellt wurden. Inlinerichtlinie:

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Action": [
                "sts:AssumeRole"
            ],
            "Resource": [
                "arn:aws:iam::*:role/AWSControlTowerExecution"
            ],
            "Effect": "Allow"
        }
    ]
}
```

Vertrauensrichtlinie

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudformation.amazonaws.com"
```

```
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

AWS ControlTowerCloudTrailRolePolicy

AWS Control Tower ermöglicht dies CloudTrail als bewährte Methode und bietet diese Rolle an CloudTrail. CloudTrail übernimmt diese Rolle beim Erstellen und Veröffentlichen von CloudTrail Protokollen.

Verwaltete Richtlinie: `AWS ControlTowerCloudTrailRolePolicy`

Diese Rolle verwendet die AWS-managed-RichtlinieAWS `ControlTowerCloudTrailRolePolicy`, die die erforderlichen Berechtigungen gewährt CloudTrail , um Auditprotokolle im Auftrag von AWS Control Tower in Amazon CloudWatch Logs zu veröffentlichen. Diese verwaltete Richtlinie ersetzt die Inline-Richtlinie, die zuvor für diese Rolle verwendet wurde, sodass AWS die Richtlinie ohne Eingreifen des Kunden aktualisiert werden kann.

Weitere Informationen finden Sie AWS ControlTowerCloudTrailRolePolicy im AWS Managed Policy Reference Guide.

Aktualisierungen dieser verwalteten Richtlinie sind in der Tabelle zusammengefasstVerwaltete Richtlinien für AWS Control Tower.

> **Note**
>
> Vor der Einführung der verwalteten Richtlinie verwendete diese Rolle eine integrierte Richtlinie mit entsprechenden Berechtigungen. Die Inline-Richtlinie wurde durch die verwaltete Richtlinie ersetzt, um reibungslose Aktualisierungen zu ermöglichen.

Frühere Inline-Richtlinie (als Referenz):

JSON

```
{
```

```
    "Version":"2012-10-17",
    "Statement": [
        {
            "Action": "logs:CreateLogStream",
            "Resource": "arn:aws:logs:*:*:log-group:aws-controltower/
CloudTrailLogs:*",
            "Effect": "Allow"
        },
        {
            "Action": "logs:PutLogEvents",
            "Resource": "arn:aws:logs:*:*:log-group:aws-controltower/
CloudTrailLogs:*",
            "Effect": "Allow"
        }
    ]
}
```

Vertrauensrichtlinie

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudtrail.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

AWS ControlTowerBlueprintAccess Anforderungen an die Rolle

Für AWS Control Tower müssen Sie die `AWS ControlTowerBlueprintAccess` Rolle im angegebenen Blueprint-Hub-Konto innerhalb derselben Organisation erstellen.

Name der Rolle

Der Rollenname muss lauten. `AWS ControlTowerBlueprintAccess`

Richtlinie zum Vertrauen in die Rolle

Die Rolle muss so eingerichtet sein, dass sie den folgenden Prinzipien vertraut:

- Der Principal, der AWS Control Tower im Verwaltungskonto verwendet.
- Die `AWS ControlTowerAdmin` Rolle im Verwaltungskonto.

Das folgende Beispiel zeigt eine Vertrauensrichtlinie mit den geringsten Rechten. Wenn Sie Ihre eigene Richtlinie erstellen, ersetzen Sie den Begriff *`YourManagementAccountId`* durch die tatsächliche Konto-ID Ihres AWS Control Tower-Managementkontos und den Begriff *`YourControlTowerUserRole`* durch die ID der IAM-Rolle für Ihr Verwaltungskonto.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": [
                    "arn:aws:iam::111122223333:role/service-role/
AWSControlTowerAdmin",
                    "arn:aws:iam::111122223333:role/YourControlTowerUserRole"
                ]
            },
            "Action": "sts:AssumeRole",
            "Condition": {}
        }
    ]
}
```

Berechtigungen für Rollen

Sie müssen die verwaltete Richtlinie AWSServiceCatalogAdminFullAccess an die Rolle anhängen.

AWSServiceRoleForAWSControlTower

Diese Rolle gewährt AWS Control Tower Zugriff auf das Log Archive-Konto, das Audit-Konto und die Mitgliedskonten für Operationen, die für die Wartung der Landezone von entscheidender Bedeutung sind, z. B. um Sie über ungenutzte Ressourcen zu informieren.

Die `AWS ServiceRoleFor AWS ControlTower` Rolle erfordert eine angefügte verwaltete Richtlinie und eine Rollenvertrauensrichtlinie für die IAM-Rolle.

Verwaltete Richtlinie für diese Rolle: `AWS ControlTowerAccountServiceRolePolicy`

Richtlinie zur Vertrauensstellung für die Rolle:

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "controltower.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

AWS ControlTowerAccountServiceRolePolicy

Diese AWS verwaltete Richtlinie ermöglicht es AWS Control Tower, AWS Dienste aufzurufen, die eine automatische Kontokonfiguration und zentrale Verwaltung in Ihrem Namen ermöglichen.

Die Richtlinie enthält die Mindestberechtigungen für AWS Control Tower, um die Weiterleitung von AWS Security Hub CSPM Ergebnissen für Ressourcen zu implementieren, die von Security Hub CSPM-Kontrollen verwaltet werden, die Teil des Security Hub Service-managed CSPM-Standards sind: AWS Control Tower, und sie verhindert Änderungen, die die Verwaltung von Kundenkonten einschränken. Es ist Teil des Prozesses zur Erkennung von AWS Security Hub CSPM Abweichungen im Hintergrund, der nicht direkt vom Kunden initiiert wird.

Die Richtlinie gewährt die Erlaubnis, EventBridge Amazon-Regeln, speziell für Security Hub CSPM-Kontrollen, in jedem Mitgliedskonto zu erstellen, und diese Regeln müssen eine genaue Angabe enthalten. EventPattern Außerdem kann eine Regel nur auf Regeln angewendet werden, die von unserem Service Principal verwaltet werden.

Servicemitarbeiter: `controltower.amazonaws.com`

Weitere Informationen finden Sie AWS ControlTowerAccountServiceRolePolicy im AWS Managed Policy Reference Guide.

Aktualisierungen dieser verwalteten Richtlinie sind in der Tabelle zusammengefasstVerwaltete Richtlinien für AWS Control Tower.

Verwaltete Richtlinien für AWS Control Tower

AWS deckt viele gängige Anwendungsfälle ab, indem eigenständige IAM-Richtlinien bereitgestellt werden, die von erstellt und verwaltet werden. AWS Die verwalteten Richtlinien erteilen die erforderlichen Berechtigungen für viele häufige Anwendungsfälle, sodass Sie nicht mühsam ermitteln müssen, welche Berechtigungen erforderlich sind. Weitere Informationen finden Sie unter AWS - verwaltete Richtlinien im IAM-Benutzerhandbuch.

Änderungen	Beschreibung	Datum
AWS ControlTowerServiceRolePolicy – Aktualisierung auf eine bestehende Richtlinie	AWS Control Tower hat die `cloudformation:BatchDescribeTypeConfigurations` Berechtigung von der ressourcenspezifischen Hooks-Anweisung in eine neue Anweisung mit verschoben`Resource: "*"`, da Berechtigungen auf Ressourcenebene für diese API CloudFormation nicht unterstützt werden.	19. Mai 2026
AWS ControlTowerAccountServiceRolePolicy – Aktualisi	AWS Control Tower hat neue Berechtigungen hinzugefügt, die es AWS Control Tower	19. Mai 2026

Änderungen	Beschreibung	Datum
erung auf eine bestehende Richtlinie	ermöglichen, Aufrufe an die AWS CloudFormation Service-API `BatchDescribeTypeConfigurations` zu tätigen, um eine interne Verbesserung der serviceverknüpften Hooks vorzunehmen.	
AWS ControlTowerAccountServiceRolePolicy – Aktualisierung auf eine bestehende Richtlinie	AWS Control Tower hat eine bestehende Richtlinie aktualisiert, um die Validierungspräzision für EventBridge Amazon-Regelbedingungen zu verbessern. Das Update verschiebt die `events:detail-type` Bedingung von 1 `StringEquals` auf, `ForAllValues:StringEquals` um eine bessere Kontrolle über den Abgleich von Ereignismustern zu gewährleisten und gleichzeitig die gleichen funktionalen Berechtigungen beizubehalten.	30. Dezember 2025

Änderungen	Beschreibung	Datum
AWS ControlTowerAccountServiceRolePolicy – Aktualisierung auf eine bestehende Richtlinie	AWS Control Tower hat eine neue Richtlinie hinzugefügt, die die folgenden Berechtigungen erweitert: • AWS Config Berechtigungen zum Erstellen, Markieren, Löschen, Verwalten und Lesen eines serviceverknüpften Konfigurationsaggregators • AWS Config Berechtigungen zur Beschreibung aller Konfigurationsaggregatoren • AWS Organizations Erlaubnis, delegierte Administratoren aufzulisten für AWS Config • AWS Organizations Erlaubnis, die Organisation zu beschreiben • CloudFormation Berechtigungen zur Verwaltung dienstbezogener Hooks	10. November 2025

Änderungen	Beschreibung	Datum
AWS ControlTowerServiceRolePolicy— Aktualisierte verwaltete Richtlinie	AWS Control Tower hat das Amazon CloudWatch Logs-Ressourcenmuster aktualisiert, AWS ControlTowerServiceRolePolicy um die optionale AWS CloudTrail Integration von Landing Zone 4.0 zu unterstützen. Das Muster wurde von `aws-controltower/CloudTrailLogs:*` zu geändert. Danach wurde ein Platzhalterzeichen hinzugefügtaws-controltower/`CloudTrailLogs*:*` , `CloudTrailLogs` um die Verwaltung von Protokollgruppen mit einem beliebigen Suffix zu ermöglichen. Dieses Update ermöglicht die optionale AWS CloudTrail Integration von Landing Zone 4.0, die es Kunden ermöglicht, die AWS CloudTrail Integration mehrfach zu aktivieren und zu deaktivieren. Jedes Mal, wenn die Integration aktiviert wird, werden Amazon CloudWatch Logs-Protokollgruppen mit eindeutigen Suffixen neu erstellt, um Namenskonflikte zu vermeiden. Das Update ist abwärtsko	31. Oktober 2025

Änderungen	Beschreibung	Datum
	mpatibel mit vorhandenen Bereitstellungen.	
AWS ControlTowerCloudTrailRolePolicy— Neue verwaltete Richtlinie	AWS Control Tower führte die AWS ControlTowerCloudTrailRolePolicy verwaltete Richtlinie ein, die es ermöglicht, Log-Streams CloudTrail zu erstellen und Protokollereignisse in den Control Tower-managed Amazon CloudWatch Logs-Protokollgruppen zu veröffentlichen. Diese verwaltete Richtlinie ersetzt die zuvor von der verwendete Inline-Richtlinie und ermöglicht es AWS ControlTowerCloudTrailRole, die Richtlinie ohne Eingreifen des Kunden AWS zu aktualisieren. Die Richtlinie ist auf Protokollgruppen beschränkt, deren Namen dem Muster entsprechen. `aws-controltower/CloudTrailLogs*`	31. Oktober 2025

Änderungen	Beschreibung	Datum
AWS ControlTowerIdentityCenterManagementPolicy— Eine neue Richtlinie	AWS Control Tower hat eine neue Richtlinie hinzugefügt, die es Kunden ermöglicht, IAM Identity Center-Ressourcen in Konten zu konfigurieren, die bei AWS Control Tower registriert sind, und sie ermöglicht es AWS Control Tower, einige Arten von Abweichungen bei der automatischen Registrierung von Konten zu beheben. Diese Änderung ist erforderlich, damit Kunden das IAM Identity Center im AWS Control Tower konfigurieren können und AWS Control Tower die automatische Registrierung korrigieren kann.	10. Oktober 2025
AWS ControlTowerServiceRolePolicy – Aktualisierung auf eine bestehende Richtlinie	AWS Control Tower hat neue CloudFormation Berechtigungen hinzugefügt, die es AWS Control Tower ermöglichen, Stack-Set-Ressourcen abzufragen und für Mitgliedskonten bereitzustellen, wenn die Konten automatisch bei AWS Control Tower registriert werden.	10. Oktober 2025

Änderungen	Beschreibung	Datum
AWS ControlTowerServiceRolePolicy – Aktualisierung auf eine bestehende Richtlinie	AWS Control Tower hat neue Berechtigungen hinzugefügt, die es Kunden ermöglichen, serviceverknüpfte AWS Config Regeln zu aktivieren und zu deaktivieren. Diese Änderung ist erforderlich, damit Kunden Kontrollen verwalten können, die anhand von Config-Regeln bereitgestellt werden.	5. Juni 2025
AWS ControlTowerServiceRolePolicy – Aktualisierung auf eine bestehende Richtlinie	AWS Control Tower hat neue Berechtigungen hinzugefügt, die es AWS Control Tower ermöglichen, Aufrufe an die AWS CloudFormation Service-APIs zu tätigen `ActivateType` `DeactivateType` , und`SetTypeConfiguration` , weiter`AWS::ControlTower` `types` . Diese Änderung ermöglicht es Kunden, proaktive Kontrollen bereitzustellen, ohne private CloudFormation Hook-Typen einsetzen zu müssen.	10. Dezember 2024

Änderungen	Beschreibung	Datum
AWS ControlTowerAccountServiceRolePolicy— Eine neue Richtlinie	AWS Control Tower hat eine neue serviceverknüpfte Rolle hinzugefügt, die es AWS Control Tower ermöglicht, Ereignisregeln zu erstellen und zu verwalten und auf der Grundlage dieser Regeln die Drift-Erkennung für Kontrollen zu verwalten, die sich auf Security Hub CSPM beziehen. Diese Änderung ist erforderlich, damit Kunden auf der Konsole abgelenkte Ressourcen sehen können, wenn sich diese Ressourcen auf Security Hub CSPM-Steuerelemente beziehen, die Teil des Security Hub CSPM-Standards sind: AWS Control Tower. Service-managed	22. Mai 2023

Änderungen	Beschreibung	Datum
AWS ControlTowerServiceRolePolicy – Aktualisierung auf eine bestehende Richtlinie	AWS Control Tower hat neue Berechtigungen hinzugefügt, die es AWS Control Tower ermöglichen `EnableRegion` `ListRegions` , Aufrufe an die und vom AWS Account Management Service implementierten `GetRegionOptStatus` APIs zu tätigen, um das Opt-In für Kundenkonten in der Landing Zone AWS-Regionen verfügbar zu machen (Verwaltungskonto, Protokollarchivkonto, Auditkonto, OU-Mitgliedskonten). Diese Änderung ist erforderlich, damit Kunden die Option haben, die Region-Governance durch AWS Control Tower auf die Opt-in-Regionen auszudehnen.	06. April 2023

Änderungen	Beschreibung	Datum
AWS ControlTowerServiceRolePolicy – Aktualisierung auf eine bestehende Richtlinie	AWS Control Tower hat neue Berechtigungen hinzugefügt, die es AWS Control Tower ermöglichen, die `AWSControlTowerBlueprintAccess` Rolle im Blueprint-Konto (Hub-Konto) zu übernehmen. Dabei handelt es sich um ein dediziertes Konto in einer Organisation, das vordefinierte Blueprints enthält, die in einem oder mehreren Service Catalog-Produkten gespeichert sind. AWS Control Tower übernimmt die `AWSControlTowerBlueprintAccess` Aufgabe, drei Aufgaben auszuführen: ein Service Catalog-Portfolio erstellen, das angeforderte Blueprint-Produkt hinzufügen und das Portfolio zum Zeitpunkt der Kontobereitstellung für ein angefordertes Mitgliedskonto freigeben. Diese Änderung ist erforderlich, damit Kunden benutzerdefinierte Konten über AWS Control Tower Account Factory bereitstellen können.	28. Oktober 2022

Änderungen	Beschreibung	Datum
AWS ControlTowerServiceRolePolicy – Aktualisierung auf eine bestehende Richtlinie	AWS Control Tower hat ab Version 3.0 der Landing Zone neue Berechtigungen hinzugefügt, die es Kunden ermöglichen, AWS CloudTrail Trails auf Organisationsebene einzurichten. Die organisationsbasierte CloudTrail Funktion erfordert , dass Kunden den vertrauen swürdigen Zugriff für den CloudTrail Service aktiviert haben, und der IAM-Benut zer oder die IAM-Rolle muss die Berechtigung haben, im Verwaltungskonto einen Trail auf Organisationsebene zu erstellen.	20. Juni 2022

Änderungen	Beschreibung	Datum
AWS ControlTowerServiceRolePolicy – Aktualisierung auf eine bestehende Richtlinie	AWS Control Tower hat neue Berechtigungen hinzugefügt, die es Kunden ermöglichen, die KMS-Schlüsselverschlüsselung zu verwenden. Die KMS-Funktion ermöglicht es Kunden, ihren eigenen KMS-Schlüssel zum Verschlüsseln ihrer CloudTrail Protokolle bereitzustellen. Kunden können den KMS-Schlüssel auch während der Aktualisierung oder Reparatur der Landezone ändern. Beim Aktualisieren des KMS-Schlüssels sind AWS CloudFormation Berechtigungen zum Aufrufen der AWS CloudTrail `PutEventSelector` API erforderlich. Die Änderung an der Richtlinie besteht darin, dass die AWS ControlTowerAdmin Rolle die AWS CloudTrail `PutEventSelector` API aufrufen kann.	28. Juli 2021
AWS Control Tower hat begonnen, Änderungen zu verfolgen	AWS Control Tower hat damit begonnen, Änderungen für die von AWS ihm verwalteten Richtlinien zu verfolgen.	27. Mai 2021

Sicherheit im AWS Control Tower

Cloud-Sicherheit AWS hat höchste Priorität. Als AWS Kunde profitieren Sie von einer Rechenzentrums- und Netzwerkarchitektur, die darauf ausgelegt sind, die Anforderungen der sicherheitssensibelsten Unternehmen zu erfüllen.

Sicherheit ist eine gemeinsame Verantwortung von Ihnen AWS und Ihnen. Im Modell der übergreifenden Verantwortlichkeit wird Folgendes mit „Sicherheit der Cloud“ bzw. „Sicherheit in der Cloud“ umschrieben:

- Sicherheit der Cloud — AWS ist verantwortlich für den Schutz der Infrastruktur, die AWS Dienste in der AWS Cloud ausführt. AWS bietet Ihnen auch Dienste, die Sie sicher nutzen können. Die Wirksamkeit unserer Sicherheitsfunktionen wird regelmäßig von externen Prüfern im Rahmen des AWS -Compliance-Programms getestet und überprüft. Weitere Informationen zu den Compliance-Programmen, die für AWS Control Tower gelten, finden Sie unter AWS Services in Scope by Compliance Program.
- Sicherheit in der Cloud — Ihre Verantwortung hängt von den AWS Services ab, die Sie nutzen. In Ihre Verantwortung fallen außerdem weitere Faktoren, wie z. B. die Vertraulichkeit der Daten, die Anforderungen Ihrer Organisation sowie geltende Gesetze und Vorschriften.

Diese Dokumentation hilft Ihnen zu verstehen, wie Sie das Modell der gemeinsamen Verantwortung bei der Verwendung von AWS Control Tower anwenden können. In den folgenden Themen erfahren Sie, wie Sie AWS Control Tower konfigurieren, um Ihre Sicherheits- und Compliance-Ziele zu erreichen. Sie erfahren auch, wie Sie andere AWS Services nutzen können, mit denen Sie Ihre AWS Control Tower Tower-Ressourcen überwachen und sichern können.

Datenschutz in AWS Control Tower

Das AWS Modell der gilt für den Datenschutz in AWS Control Tower. Wie in diesem Modell beschrieben, AWS ist verantwortlich für den Schutz der globalen Infrastruktur, auf der alle Systeme laufen AWS Cloud. Sie sind dafür verantwortlich, die Kontrolle über Ihre in dieser Infrastruktur gehosteten Inhalte zu behalten. Sie sind auch für die Sicherheitskonfiguration und die Verwaltungsaufgaben für die von Ihnen verwendeten AWS-Services verantwortlich. Weitere Informationen zum Datenschutz finden Sie unter Häufig gestellte Fragen zum Datenschutz . Weitere Informationen zum Datenschutz in Europa finden Sie im Zentrum für die Datenschutz-Grundverordnung (DSGVO).

Aus Datenschutzgründen empfehlen wir, dass Sie AWS-Konto Anmeldeinformationen schützen und einzelne Benutzer mit AWS IAM Identity Center oder AWS Identity and Access Management (IAM) einrichten. So erhält jeder Benutzer nur die Berechtigungen, die zum Durchführen seiner Aufgaben erforderlich sind. Außerdem empfehlen wir, die Daten mit folgenden Methoden schützen:

- Verwenden Sie für jedes Konto die Multi-Faktor-Authentifizierung (MFA).
- Wird verwendet SSL/TLS , um mit AWS Ressourcen zu kommunizieren. Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Richten Sie die API und die Protokollierung von Benutzeraktivitäten mit ein AWS CloudTrail. Informationen zur Verwendung von CloudTrail Pfaden zur Erfassung von AWS Aktivitäten finden Sie unter Arbeiten mit CloudTrail Pfaden im AWS CloudTrail Benutzerhandbuch.
- Verwenden Sie AWS Verschlüsselungslösungen zusammen mit allen darin enthaltenen Standardsicherheitskontrollen AWS-Services.
- Verwenden Sie erweiterte verwaltete Sicherheitsservices wie Amazon Macie, die dabei helfen, in Amazon S3 gespeicherte persönliche Daten zu erkennen und zu schützen.
- Wenn Sie für den Zugriff AWS über eine Befehlszeilenschnittstelle oder eine API FIPS 140-3-validierte kryptografische Module benötigen, verwenden Sie einen FIPS-Endpunkt. Weitere Informationen über verfügbare FIPS-Endpunkte finden Sie unter Federal Information Processing Standard (FIPS) 140-3.

Wir empfehlen dringend, in Freitextfeldern, z. B. im Feld Name, keine vertraulichen oder sensiblen Informationen wie die E-Mail-Adressen Ihrer Kunden einzugeben. Dies gilt auch, wenn Sie mit AWS Control Tower oder anderen Geräten arbeiten und die Konsole AWS CLI, API oder AWS SDKs AWS-Services verwenden. Alle Daten, die Sie in Tags oder Freitextfelder eingeben, die für Namen verwendet werden, können für Abrechnungs- oder Diagnoseprotokolle verwendet werden. Wenn Sie eine URL für einen externen Server bereitstellen, empfehlen wir dringend, keine Anmeldeinformationen zur Validierung Ihrer Anforderung an den betreffenden Server in die URL einzuschließen.

> **Note**
>
> Die Protokollierung von Benutzeraktivitäten mit AWS CloudTrail erfolgt automatisch in AWS Control Tower, wenn Sie Ihre landing zone einrichten.

Weitere Informationen zum Datenschutz enthält der Blog-Beitrag AWS Shared Responsibility Model and GDPR im AWS -Sicherheitsblog. AWS Control Tower bietet die folgenden Optionen, mit denen Sie die Inhalte schützen können, die in Ihrer landing zone vorhanden sind:

Themen

- Verschlüsselung im Ruhezustand
- Verschlüsselung während der Übertragung
- Einschränken des Zugriffs auf Inhalte

Verschlüsselung im Ruhezustand

AWS Control Tower verwendet Amazon S3 S3-Buckets und Amazon DynamoDB DynamoDB-Datenbanken, die im Ruhezustand mithilfe von Amazon S3-Managed Keys (SSE-S3) zur Unterstützung Ihrer landing zone verschlüsselt werden. Diese Verschlüsselung wird standardmäßig konfiguriert, wenn Sie Ihre landing zone einrichten. Optional können Sie Ihre landing zone so konfigurieren, dass Ressourcen mit KMS-Verschlüsselungsschlüsseln verschlüsselt werden. Sie können auch eine Verschlüsselung im Ruhezustand für die Dienste einrichten, die Sie in Ihrer landing zone für die Dienste verwenden, die sie unterstützen. Weitere Informationen finden Sie im Kapitel Sicherheit der Online-Dokumentation zu diesem Dienst.

Verschlüsselung während der Übertragung

AWS Control Tower verwendet Transport Layer Security (TLS) und clientseitige Verschlüsselung für die Verschlüsselung bei der Übertragung zur Unterstützung Ihrer landing zone. Darüber hinaus erfordert der Zugriff auf AWS Control Tower die Verwendung der Konsole, auf die nur über einen HTTPS-Endpunkt zugegriffen werden kann. Diese Verschlüsselung wird standardmäßig konfiguriert, wenn Sie Ihre landing zone einrichten.

Einschränken des Zugriffs auf Inhalte

Als bewährte Methode sollten Sie den Zugriff auf die entsprechenden Benutzergruppen einschränken. Mit AWS Control Tower können Sie dies tun, indem Sie sicherstellen, dass Ihre zentralen Cloud-Administratoren und Endbenutzer über die richtigen IAM-Berechtigungen verfügen oder, im Fall von IAM Identity Center-Benutzern, dass sie sich in den richtigen Gruppen befinden.

- Weitere Informationen zu Rollen und Richtlinien für IAM-Entitäten finden Sie im IAM-Benutzerhandbuch.

- Weitere Informationen zu den IAM Identity Center-Gruppen, die bei der Einrichtung Ihrer landing zone erstellt werden, finden Sie unterIAM Identity Center-Gruppen für AWS Control Tower.

Konformitätsvalidierung für AWS Control Tower

AWS Control Tower ist ein gut durchdachter Service, der Ihrem Unternehmen mit Kontrollen und bewährten Methoden helfen kann, Ihre Compliance-Anforderungen zu erfüllen. Darüber hinaus bewerten externe Prüfer die Sicherheit und Konformität einer Reihe von Diensten, die Sie in Ihrer landing zone im Rahmen mehrerer AWS Compliance-Programme nutzen können. Hierzu zählen unter anderem SOC, PCI, FedRAMP und HIPAA.

Eine Liste der AWS Services im Rahmen bestimmter Compliance-Programme finden Sie unter AWS Services im Umfang der einzelnen Compliance-Programme. Allgemeine Informationen finden Sie unter AWS -Compliance-Programme.

Sie können Prüfberichte von Drittanbietern unter herunterladen AWS Artifact. Weitere Informationen finden Sie im AWS Artifact Benutzerhandbuch unter Herunterladen von Berichten in AWS Artifact.

Ihre Compliance-Verantwortung bei der Nutzung von AWS Control Tower hängt von der Sensibilität Ihrer Daten, den Compliance-Zielen Ihres Unternehmens und den geltenden Gesetzen und Vorschriften ab. AWS bietet die folgenden Ressourcen zur Unterstützung bei der Einhaltung von Vorschriften:

- Schnellstartanleitungen zu Sicherheit und Compliance — In diesen Bereitstellungsleitfäden werden architektonische Überlegungen erörtert und Schritte für die Implementierung von Umgebungen beschrieben, auf denen auf Sicherheit und Compliance ausgerichtete Basisumgebungen eingerichtet werden. AWS
- Architektur für HIPAA-Sicherheit und -Compliance auf Amazon Web Services — In diesem Whitepaper wird beschrieben, wie Unternehmen Anwendungen erstellen können AWS . HIPAA-compliant
- AWS Ressourcen zur Einhaltung von Vorschriften — Diese Sammlung von Arbeitsmappen und Leitfäden kann auf Ihre Branche und Ihren Standort zutreffen.
- AWS Config— Mit diesem AWS Service wird bewertet, wie gut Ihre Ressourcenkonfigurationen den internen Praktiken, Branchenrichtlinien und Vorschriften entsprechen.
- AWS Security Hub CSPM— Dieser AWS Service bietet einen umfassenden Überblick über Ihren Sicherheitsstatus und hilft Ihnen AWS , die Einhaltung der Sicherheitsstandards und bewährten Verfahren der Sicherheitsbranche zu überprüfen.

Ausfallsicherheit im AWS Control Tower

Die AWS globale Infrastruktur basiert auf AWS Regionen und Availability Zones.

AWS Regionen bieten mehrere physisch getrennte und isolierte Availability Zones, die über Netzwerke mit niedriger Latenz, hohem Durchsatz und hoher Redundanz miteinander verbunden sind. Mithilfe von Availability Zones können Sie Anwendungen und Datenbanken erstellen und ausführen, die automatisch Failover zwischen Availability Zones ausführen, ohne dass es zu Unterbrechungen kommt. Availability Zones sind besser hoch verfügbar, fehlertoleranter und skalierbarer als herkömmliche Infrastrukturen mit einem oder mehreren Rechenzentren.

Eine Liste, AWS-Regionen wo AWS Control Tower verfügbar ist, finden Sie unterWie AWS Regionen arbeiten mit AWS Control Tower.

Ihre Heimatregion ist definiert als die AWS Region, in der Ihre landing zone eingerichtet wurde.

Weitere Informationen zu AWS Regionen und Availability Zones finden Sie unter AWS Globale Infrastruktur.

Infrastruktursicherheit in AWS Control Tower

AWS Control Tower ist durch die AWS globalen Netzwerksicherheitsverfahren geschützt, die im Whitepaper Amazon Web Services: Sicherheitsprozesse im Überblick beschrieben sind.

Sie verwenden AWS veröffentlichte API-Aufrufe für den Zugriff auf AWS Dienste und Ressourcen innerhalb Ihrer landing zone über das Netzwerk. Wir benötigen Transport Layer Security (TLS) 1.2 und empfehlen Transport Layer Security (TLS) 1.3 oder höher. Kunden müssen außerdem Cipher Suites mit Perfect Forward Secrecy (PFS) wie Ephemeral (DHE) oder Elliptic Curve Ephemeral Diffie-Hellman (ECDHE) unterstützen. Diffie-Hellman Die meisten modernen Systemen wie Java 7 und höher unterstützen diese Modi.

Außerdem müssen Anforderungen mit einer Zugriffsschlüssel-ID und einem geheimen Zugriffsschlüssel signiert sein, der einem IAM-Prinzipal zugeordnet ist. Alternativ können Sie mit AWS -Security-Token-Service (AWS STS) temporäre Sicherheitsanmeldeinformationen erstellen, um die Anforderungen zu signieren.

Sie können Sicherheitsgruppen einrichten, um zusätzliche Netzwerkinfrastruktursicherheit für Ihre AWS Control Tower Tower-Landing Zone-Workloads zu gewährleisten. Weitere Informationen finden

Sie unter Exemplarische Vorgehensweise: Einrichten von Sicherheitsgruppen im AWS Control Tower mit AWS Firewall Manager.

Protokollierung und Überwachung in AWS Control Tower

Mit der Überwachung können Sie potenzielle Vorfälle einplanen und entsprechend darauf reagieren. Die Ergebnisse der Überwachungsaktivitäten werden in Protokolldateien gespeichert. Daher sind Protokollierung und Überwachung eng miteinander verbundene Konzepte, und sie sind ein wichtiger Bestandteil der gut durchdachten Architektur von AWS Control Tower.

Wenn Sie Ihre landing zone einrichten, ist eines der erstellten gemeinsamen Konten das Log-Archiv-Konto. Es dient der zentralen Erfassung aller Protokolle, einschließlich der Protokolle für all Ihre gemeinsamen Konten und Mitgliedskonten. Protokolldateien werden in einem Amazon S3 S3-Bucket gespeichert. Diese Protokolldateien ermöglichen es Administratoren und Prüfern, aufgetretene Aktionen und Ereignisse zu überprüfen.

Als bewährte Methode sollten Sie Überwachungsdaten aus allen Teilen Ihres AWS Setups in Ihren Protokollen sammeln, damit Sie einen Fehler an mehreren Stellen leichter debuggen können, falls einer auftritt. AWS bietet verschiedene Tools zur Überwachung Ihrer Ressourcen und Aktivitäten in Ihrer landing zone.

Beispielsweise wird der Status Ihrer Steuerungen ständig überwacht. Sie können ihren Status auf einen Blick in der AWS Control Tower Tower-Konsole oder programmgesteuert mithilfe der AWS Control Tower Tower-APIs sehen. Der Zustand und der Status der Konten, die Sie in Account Factory bereitgestellt haben, werden ebenfalls ständig überwacht.

Zeigen Sie protokollierte Aktionen auf der Seite Aktivitäten an

In der AWS Control Tower Tower-Konsole bietet die Seite Aktivitäten einen Überblick über die Aktionen des AWS Control Tower Tower-Managementkontos. Um zur Seite AWS Control Tower Tower-Aktivitäten zu navigieren, wählen Sie in der linken Navigationsleiste Aktivitäten aus.

Die auf der Seite Aktivitäten angezeigten Aktivitäten sind dieselben, die im AWS CloudTrail Ereignisprotokoll für AWS Control Tower gemeldet wurden, sie werden jedoch in einem Tabellenformat angezeigt. Wenn Sie mehr über eine bestimmte Aktivität erfahren möchten, wählen Sie die Aktivität aus der Tabelle aus und wählen Sie dann View details (Details anzeigen).

Sie können die Aktionen und Ereignisse der Mitgliedskonten in den Protokolldateien einsehen.

In den folgenden Abschnitten werden die Überwachung und Protokollierung in AWS Control Tower detaillierter beschrieben:

Topics

- Integrierte Tools für die Überwachung
- Protokollierung von AWS Control Tower-Aktionen mit AWS CloudTrail
- Lebenszyklusereignisse im AWS Control Tower
- Verwenden AWS Benutzerbenachrichtigungen mit AWS Control Tower

Über die Anmeldung bei AWS Control Tower

AWS Control Tower führt die Protokollierung von Aktionen und Ereignissen durch die Integration mit AWS CloudTrail und AWS Config automatisch durch und zeichnet sie auf CloudWatch. Alle Aktionen werden protokolliert, einschließlich Aktionen aus dem AWS Control Tower Tower-Verwaltungskonto und den Mitgliedskonten Ihrer Organisation. Aktionen und Ereignisse des Verwaltungskontos können auf der Seite Aktivitäten in der Konsole eingesehen werden. Sie können die Aktionen und Ereignisse der Mitgliedskonten in den Protokolldateien einsehen.

Organization-level Wanderwege

AWS Control Tower richtet einen neuen CloudTrail Trail ein, wenn Sie eine landing zone einrichten. Es handelt sich um einen Trail auf Organisationsebene, was bedeutet, dass alle Ereignisse für das Verwaltungskonto und alle Mitgliedskonten in der Organisation protokolliert werden. Diese Funktion stützt sich auf vertrauenswürdigen Zugriff, um dem Verwaltungskonto die Erlaubnis zu erteilen, für jedes Mitgliedskonto einen Trail zu erstellen.

Weitere Informationen zu AWS Control Tower und CloudTrail Organisationspfaden finden Sie unter Einen Trail für eine Organisation erstellen.

> **Note**
>
> In AWS Control Tower-Versionen vor landing zone Version 3.0 hat AWS Control Tower in jedem Konto einen Mitgliedskonten-Trail erstellt. Wenn Sie auf Version 3.0 aktualisieren, wird Ihr CloudTrail Trail zu einem Organisationspfad. Bewährte Methoden für den Wechsel zwischen Wanderwegen finden Sie im CloudTrail Benutzerhandbuch unter Bewährte Methoden für den Wegewechsel.

Wenn Sie ein Konto bei AWS Control Tower registrieren, unterliegt Ihr Konto dem AWS CloudTrail Pfad für die AWS Control Tower Tower-Organisation. Wenn Sie in diesem Konto bereits einen

CloudTrail Trail bereitgestellt haben, werden möglicherweise doppelte Gebühren angezeigt, es sei denn, Sie löschen den vorhandenen Trail für das Konto, bevor Sie ihn bei AWS Control Tower registrieren.

> **Note**
>
> Wenn Sie auf landing zone Version 3.0 aktualisieren, löscht AWS Control Tower in Ihrem Namen die Trails auf Kontoebene (die AWS Control Tower erstellt hat) in Ihren registrierten Konten. Ihre vorhandenen Protokolldateien auf Kontoebene werden in ihrem Amazon S3 S3-Bucket aufbewahrt.

Amazon S3 S3-Bucket-Richtlinie für die Protokollierung

In AWS Control Tower haben AWS Services nur dann Zugriff auf Ihre Ressourcen, wenn die Anfrage von Ihrer Organisation oder Organisationseinheit (OU) stammt. Für Schreibberechtigungen muss eine `aws:SourceOrgID` Bedingung erfüllt sein.

Sie können den `aws:SourceOrgID` Bedingungsschlüssel verwenden und den Wert auf Ihre Organisations-ID im Bedingungselement Ihrer Amazon S3 S3-Bucket-Richtlinie setzen. Diese Bedingung stellt sicher, dass nur Konten innerhalb Ihrer Organisation Protokolle in Ihren Amazon S3 S3-Bucket schreiben können. Es verhindert, dass Konten außerhalb Ihrer Organisation Protokolle in Ihren Amazon S3 S3-Bucket von AWS Control Tower schreiben.

Weitere Informationen zu diesem Bedingungsschlüssel finden Sie unter Kontext-Schlüssel für globale IAM-Bedingungen. Einen Blogbeitrag zu skalierbaren Steuerelementen finden Sie unter Verwenden skalierbarer Steuerelemente für AWS Dienste, die auf Ihre Ressourcen zugreifen.

Diese Richtlinie hat keinen Einfluss auf die Funktionalität Ihrer vorhandenen Workloads.

Landing Zone Version 3.3 und früher

In landing zone Version 3.3 und früher stellt AWS Control Tower einen einzelnen Amazon S3 S3-Bucket im Protokollarchivkonto bereit, in dem AWS CloudTrail sowohl AWS Config Protokolle als auch gespeichert werden. Die Bucket-Richtlinie wird im folgenden Beispiel gezeigt.

```
S3AuditBucketPolicy:
    Type: AWS::S3::BucketPolicy
    Properties:
      Bucket: !Ref S3AuditBucket
```

```
      PolicyDocument:
        Version: 2012-10-17
        Statement:
          - Sid: AllowSSLRequestsOnly
            Effect: Deny
            Principal: '*'
            Action: s3:*
            Resource:
             - !Sub "arn:${AWS::Partition}:s3:::${S3AuditBucket}"
             - !Sub "arn:${AWS::Partition}:s3:::${S3AuditBucket}/*"
            Condition:
              Bool:
                aws:SecureTransport: false
          - Sid: AWSBucketPermissionsCheck
            Effect: Allow
            Principal:
              Service:
                - cloudtrail.amazonaws.com
                - config.amazonaws.com
            Action: s3:GetBucketAcl
            Resource:
              - !Sub "arn:${AWS::Partition}:s3:::${S3AuditBucket}"
          - Sid: AWSConfigBucketExistenceCheck
            Effect: Allow
            Principal:
              Service:
                - cloudtrail.amazonaws.com
                - config.amazonaws.com
            Action: s3:ListBucket
            Resource:
              - !Sub "arn:${AWS::Partition}:s3:::${S3AuditBucket}"
          - Sid: AWSBucketDeliveryForConfig
            Effect: Allow
            Principal:
              Service:
                - config.amazonaws.com
            Action: s3:PutObject
            Resource:
              - Fn::Join:
                  - ""
                  -
                    - !Sub "arn:${AWS::Partition}:s3:::"
                    - !Ref "S3AuditBucket"
                    - !Sub "/${AWSLogsS3KeyPrefix}/AWSLogs/*/*"
```

```
            Condition:
              StringEquals:
                aws:SourceOrgID: !Ref OrganizationId
          - Sid: AWSBucketDeliveryForOrganizationTrail
            Effect: Allow
            Principal:
              Service:
                - cloudtrail.amazonaws.com
            Action: s3:PutObject
            Resource: !If [IsAccountLevelBucketPermissionRequiredForCloudTrail,
                [!Sub "arn:${AWS::Partition}:s3:::${S3AuditBucket}/
${AWSLogsS3KeyPrefix}/AWSLogs/${Namespace}/*", !Sub "arn:${AWS::Partition}:s3:::
${S3AuditBucket}/${AWSLogsS3KeyPrefix}/AWSLogs/${OrganizationId}/*"],
                !Sub "arn:${AWS::Partition}:s3:::${S3AuditBucket}/
${AWSLogsS3KeyPrefix}/AWSLogs/*/*"]
            Condition:
              StringEquals:
                aws:SourceOrgID: !Ref OrganizationId
```

Landing Zone Version 4.0 und höher

AWS CloudTrail Verwenden Sie in landing zone Version 4.0 und höher separate dedizierte Amazon S3 S3-Buckets anstelle eines gemeinsam genutzten Buckets. AWS Config Der Amazon S3 S3-Bucket für AWS Config Protokolle befindet sich im AWS Config Integrationskonto (früher das Audit-Konto). Der Amazon S3 S3-Bucket für AWS CloudTrail Protokolle befindet sich im AWS CloudTrail Administratorkonto (früher das Log Archive-Konto). Weitere Informationen finden Sie unter Aktualisierungen der AWS Config.

AWS CloudTrail Bucket-Richtlinie (AWS CloudTrail Administratorkonto)

Das folgende Beispiel zeigt die im AWS CloudTrail Administratorkonto bereitgestellte AWS CloudTrail Bucket-Richtlinie:

```
S3AuditBucketPolicy:
    Type: AWS::S3::BucketPolicy
    Properties:
      Bucket: !Ref S3AuditBucket
      PolicyDocument:
        Version: 2012-10-17
        Statement:
          - Sid: AllowSSLRequestsOnly
            Effect: Deny
```

```
            Principal: '*'
            Action: s3:*
            Resource:
              - !Sub "arn:${AWS::Partition}:s3:::${S3AuditBucket}"
              - !Sub "arn:${AWS::Partition}:s3:::${S3AuditBucket}/*"
            Condition:
              Bool:
                aws:SecureTransport: false
          - Sid: AWSBucketPermissionsCheck
            Effect: Allow
            Principal:
              Service:
                - cloudtrail.amazonaws.com
            Action: s3:GetBucketAcl
            Resource:
              - !Sub "arn:${AWS::Partition}:s3:::${S3AuditBucket}"
          - Sid: AWSConfigBucketExistenceCheck
            Effect: Allow
            Principal:
              Service:
                - cloudtrail.amazonaws.com
            Action: s3:ListBucket
            Resource:
              - !Sub "arn:${AWS::Partition}:s3:::${S3AuditBucket}"
          - Sid: AWSBucketDeliveryForOrganizationTrail
            Effect: Allow
            Principal:
              Service:
                - cloudtrail.amazonaws.com
            Action: s3:PutObject
            Resource: !If [IsAccountLevelBucketPermissionRequiredForCloudTrail,
                           [!Sub "arn:${AWS::Partition}:s3:::${S3AuditBucket}/
${AWSLogsS3KeyPrefix}/AWSLogs/${Namespace}/*", !Sub "arn:${AWS::Partition}:s3:::
${S3AuditBucket}/${AWSLogsS3KeyPrefix}/AWSLogs/${OrganizationId}/*"],
                           !Sub "arn:${AWS::Partition}:s3:::${S3AuditBucket}/
${AWSLogsS3KeyPrefix}/AWSLogs/*/*"]
            Condition:
              StringEquals:
                aws:SourceOrgID: !Ref OrganizationId
```

AWS Config Bucket-Richtlinie (AWS Config Integrationskonto)

Das folgende Beispiel zeigt die im AWS Config Integrationskonto bereitgestellte AWS Config Bucket-Richtlinie:

```
ConfigS3BucketPolicy:
    Type: AWS::S3::BucketPolicy
    Properties:
      Bucket: !Ref ConfigS3Bucket
      PolicyDocument:
        Version: 2012-10-17
        Statement:
          - Sid: AllowSSLRequestsOnly
            Effect: Deny
            Principal: '*'
            Action: s3:*
            Resource:
              - !Sub "arn:${AWS::Partition}:s3:::${ConfigS3Bucket}"
              - !Sub "arn:${AWS::Partition}:s3:::${ConfigS3Bucket}/*"
            Condition:
              Bool:
                aws:SecureTransport: false
          - Sid: AWSConfigBucketPermissionsCheck
            Effect: Allow
            Principal:
              Service:
                - config.amazonaws.com
            Action: s3:GetBucketAcl
            Resource:
              - !Sub "arn:${AWS::Partition}:s3:::${ConfigS3Bucket}"
          - Sid: AWSConfigBucketExistenceCheck
            Effect: Allow
            Principal:
              Service:
                - config.amazonaws.com
            Action: s3:ListBucket
            Resource:
              - !Sub "arn:${AWS::Partition}:s3:::${ConfigS3Bucket}"
          - Sid: AWSConfigBucketDelivery
            Effect: Allow
            Principal:
              Service:
                - config.amazonaws.com
```

```
            Action: s3:PutObject
            Resource:
              - !Sub "arn:${AWS::Partition}:s3:::${ConfigS3Bucket}/
${ConfigS3KeyPrefix}/AWSLogs/*/*"
            Condition:
              StringEquals:
                aws:SourceOrgID: !Ref OrganizationId
```

Integrierte Tools für die Überwachung

Die Überwachung ist ein wichtiger Bestandteil der Aufrechterhaltung der Zuverlässigkeit, Verfügbarkeit und Leistung von AWS Control Tower und Ihren anderen AWS Lösungen. AWS bietet die folgenden Überwachungstools, um AWS Control Tower zu überwachen, zu melden, wenn etwas nicht stimmt, und gegebenenfalls automatische Maßnahmen zu ergreifen:

- Amazon CloudWatch überwacht Ihre AWS Ressourcen und die Anwendungen, auf denen Sie laufen, AWS in Echtzeit. Sie können Kennzahlen erfassen und verfolgen, benutzerdefinierte Dashboards erstellen und Alarme festlegen, die Sie benachrichtigen oder Maßnahmen ergreifen, wenn eine bestimmte Metrik einen von Ihnen festgelegten Schwellenwert erreicht. Sie können beispielsweise die CPU-Auslastung oder andere Kennzahlen Ihrer Amazon EC2 EC2-Instances CloudWatch verfolgen und bei Bedarf automatisch neue Instances starten. Weitere Informationen finden Sie im CloudWatch Amazon-Benutzerhandbuch.
- Amazon EventBridge liefert nahezu in Echtzeit einen Stream von Systemereignissen, die Änderungen an AWS Ressourcen beschreiben. EventBridge ermöglicht automatisiertes ereignisgesteuertes Rechnen, da Sie Regeln schreiben können, die auf bestimmte Ereignisse achten und automatisierte Aktionen in anderen AWS Diensten auslösen können, wenn diese Ereignisse eintreten. Weitere Informationen finden Sie im Amazon CloudWatch Events-Benutzerhandbuch.
- Mit Amazon CloudWatch Logs können Sie Ihre Protokolldateien von Amazon EC2 EC2-Instances und anderen Quellen überwachen CloudTrail, speichern und darauf zugreifen. CloudWatch Logs können Informationen in den Protokolldateien überwachen und Sie benachrichtigen, wenn bestimmte Schwellenwerte erreicht werden. Sie können Ihre Protokolldaten auch in einem sehr robusten Speicher archivieren. Weitere Informationen finden Sie im Amazon CloudWatch Logs-Benutzerhandbuch.
- AWS CloudTrailerfasst API-Aufrufe und zugehörige Ereignisse, die von oder im Namen Ihres AWS Kontos getätigt wurden, und übermittelt die Protokolldateien an einen von Ihnen angegebenen Amazon S3 S3-Bucket. Sie können feststellen, welche Benutzer und Konten angerufen wurden

AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Aufrufe erfolgten.

Tipp: Sie können die CloudTrail Aktivitäten eines Kontos über CloudWatch Logs und Logs Insights einsehen und CloudWatch abfragen. Diese Aktivität umfasst Lebenszyklusereignisse von AWS Control Tower. CloudWatch Die Funktionen von Logs ermöglichen es Ihnen, detailliertere und genauere Abfragen durchzuführen, als Sie es normalerweise tun würden. CloudTrail

Weitere Informationen finden Sie unter Protokollierung von AWS Control Tower-Aktionen mit AWS CloudTrail.

Protokollierung von AWS Control Tower-Aktionen mit AWS CloudTrail

AWS Control Tower ist in einen Service integriert AWS CloudTrail, der eine Aufzeichnung der von einem Benutzer, einer Rolle oder einem AWS Service in AWS Control Tower ergriffenen Aktionen bereitstellt. CloudTrail erfasst Aktionen für den AWS Control Tower als Ereignisse. Wenn Sie einen Trail erstellen, können Sie die kontinuierliche Übertragung von CloudTrail Ereignissen an einen Amazon S3-Bucket aktivieren, einschließlich Ereignissen für AWS Control Tower.

Auch wenn Sie keinen Trail konfigurieren, können Sie die neuesten Ereignisse in der CloudTrail-Konsole in Event history (Ereignisverlauf) anzeigen. Anhand der gesammelten Informationen von können Sie ermitteln CloudTrail, welche Anfrage an den AWS Control Tower gestellt wurde, die IP-Adresse, von der aus die Anfrage gestellt wurde, wer die Anfrage gestellt hat, wann sie gestellt wurde, und weitere Details.

Weitere Informationen CloudTrail, einschließlich der Konfiguration und Aktivierung, finden Sie im AWS CloudTrail Benutzerhandbuch.

Informationen zum AWS Control Tower finden Sie unter CloudTrail

CloudTrail ist in Ihrem AWS Konto aktiviert, wenn Sie das Konto erstellen. Wenn im AWS Control Tower eine unterstützte Ereignisaktivität auftritt, wird diese Aktivität zusammen mit anderen AWS Serviceereignissen im CloudTrail Eventverlauf in einem Ereignis aufgezeichnet. Sie können aktuelle Ereignisse in Ihrem AWS Konto anzeigen, suchen und herunterladen. Weitere Informationen finden Sie unter Ereignisse mit dem CloudTrail Eventverlauf anzeigen.

> **Note**
>
> In AWS Control Tower-Versionen vor der Landing Zone-Version 3.0 erstellte AWS Control Tower einen Mitgliedskonto-Trail. Wenn Sie auf Version 3.0 aktualisieren, wird Ihr CloudTrail Trail aktualisiert und in einen Organisationspfad umgewandelt. Bewährte Methoden für den Wechsel zwischen Pfaden finden Sie im CloudTrail Benutzerhandbuch unter Einen Organisationspfad erstellen.

Empfehlung: Erstellen Sie einen Pfad

Für eine fortlaufende Aufzeichnung der Ereignisse in Ihrem AWS Konto, einschließlich der Ereignisse für den AWS Control Tower, erstellen Sie einen Trail. Ein Trail ermöglicht CloudTrail die Übermittlung von Protokolldateien an einen Amazon S3-Bucket. Wenn Sie einen Trail in der Konsole anlegen, gilt dieser für alle AWS -Regionen. Der Trail protokolliert Ereignisse aus allen Regionen in der AWS Partition und übermittelt die Protokolldateien an den von Ihnen angegebenen Amazon S3-Bucket. Darüber hinaus können Sie andere AWS Dienste so konfigurieren, dass sie die in den CloudTrail Protokollen gesammelten Ereignisdaten weiter analysieren und darauf reagieren. Weitere Informationen finden Sie hier:

- Übersicht zum Erstellen eines Trails
- Bereite dich auf die Erstellung eines Trails vor
- Verwaltung der CloudTrail Kosten
- CloudTrail Unterstützte Dienste und Integrationen
- Konfiguration von Amazon SNS-Benachrichtigungen für CloudTrail
- Empfangen von CloudTrail Protokolldateien aus mehreren Regionen und Empfangen von CloudTrail Protokolldateien von mehreren Konten

AWS Control Tower protokolliert die folgenden Aktionen als Ereignisse in CloudTrail Protokolldateien:

Öffentliche APIs

- Eine vollständige Liste der öffentlichen APIs von AWS Control Tower und Einzelheiten zu den einzelnen APIs finden Sie unter The AWS Control Tower API Reference. Aufrufe dieser öffentlichen APIs werden von protokolliert AWS CloudTrail.

Sonstige APIs

- SetupLandingZone
- UpdateAccountFactoryConfig
- ManageOrganizationalUnit
- CreateManagedAccount
- GetLandingZoneStatus
- GetHomeRegion
- ListManagedAccounts
- DescribeManagedAccount
- DescribeAccountFactoryConfig
- DescribeGuardrailForTarget
- DescribeManagedOrganizationalUnit
- ListEnabledGuardrails
- ListGuardrailViolations
- ListGuardrails
- ListGuardrailsForTarget
- ListManagedAccountsForGuardrail
- ListManagedAccountsForParent
- ListManagedOrganizationalUnits
- ListManagedOrganizationalUnitsForGuardrail
- GetGuardrailComplianceStatus
- DescribeGuardrail
- ListDirectoryGroups
- DescribeSingleSignOn
- DescribeCoreService
- GetAvailableUpdates

Jeder Ereignis- oder Protokolleintrag enthält Informationen zu dem Benutzer, der die Anforderung generiert hat. Die Identitätsinformationen unterstützen Sie bei der Ermittlung der folgenden Punkte:

- Ob die Anfrage mit Root- oder AWS Identity and Access Management (IAM-) Benutzeranmeldeinformationen gestellt wurde.
- Gibt an, ob die Anforderung mit temporären Sicherheitsanmeldeinformationen für eine Rolle oder einen Verbundbenutzer gesendet wurde.
- Ob die Anfrage von einem anderen AWS Dienst gestellt wurde.
- Ob die Anfrage abgelehnt wurde, weil der Zugriff verweigert wurde, oder ob sie erfolgreich verarbeitet wurde.

Weitere Informationen finden Sie unter CloudTrail userIdentity-Element.

Beispiel: Einträge in der AWS Control Tower-Protokolldatei

Ein Trail ist eine Konfiguration, die die Übermittlung von Ereignissen als Protokolldateien an einen von Ihnen angegebenen Amazon S3-Bucket ermöglicht. CloudTrail Protokolldateien enthalten einen oder mehrere Protokolleinträge. Ein Ereignis stellt eine einzelne Anforderung aus einer beliebigen Quelle dar und enthält Informationen über die angeforderte Aktion, Datum und Uhrzeit der Aktion, Anforderungsparameter usw. CloudTrail Ereignisse erscheinen in den Protokolldateien nicht in einer bestimmten Reihenfolge.

Das folgende Beispiel zeigt einen CloudTrail Protokolleintrag, der die Struktur eines typischen Protokolldateieintrags für ein `SetupLandingZone` AWS Control Tower-Ereignis zeigt, einschließlich einer Aufzeichnung der Identität des Benutzers, der die Aktion initiiert hat.

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AIDACKCEVSQ6C2EXAMPLE:backend-test-assume-role-session",
    "arn": "arn:aws:sts::76543EXAMPLE;:assumed-role/AWSControlTowerTestAdmin/backend-
test-assume-role-session",
    "accountId": "76543EXAMPLE",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2018-11-20T19:36:11Z"
      },
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
```

```
        "arn": "arn:aws:iam::AKIAIOSFODNN7EXAMPLE:role/AWSControlTowerTestAdmin",
        "accountId": "AIDACKCEVSQ6C2EXAMPLE",
        "userName": "AWSControlTowerTestAdmin"
      }
    }
  },
  "eventTime": "2018-11-20T19:36:15Z",
  "eventSource": "controltower.amazonaws.com",
  "eventName": "SetupLandingZone",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "AWS Internal",
  "userAgent": "Coral/Netty4",
  "errorCode": "InvalidParametersException",
  "errorMessage": "Home region EU_CENTRAL_1 is unsupported",
  "requestParameters": {
    "homeRegion": "EU_CENTRAL_1",
    "logAccountEmail": "HIDDEN_DUE_TO_SECURITY_REASONS",
    "sharedServiceAccountEmail": "HIDDEN_DUE_TO_SECURITY_REASONS",
    "securityAccountEmail": "HIDDEN_DUE_TO_SECURITY_REASONS",
    "securityNotificationEmail": "HIDDEN_DUE_TO_SECURITY_REASONS"
  },
  "responseElements": null,
  "requestID": "96f47b68-ed5f-4268-931c-807cd1f89a96",
  "eventID": "4ef5cf08-39e5-4fdf-9ea2-b07ced506851",
  "eventType": "AwsApiCall",
  "recipientAccountId": "76543EXAMPLE"
}
```

Überwachen Sie Ressourcenänderungen mit AWS Config

AWS Control Tower AWS Config aktiviert alle registrierten Konten, sodass es die Einhaltung der Vorschriften durch detektive Kontrollen überwachen, Ressourcenänderungen aufzeichnen und Ressourcenänderungsprotokolle an ein zentrales Konto senden kann. AWS Control Tower zentralisiert diese AWS Config Daten, sodass Sie Änderungen an der Ressourcenkonfiguration aller registrierten Konten an einem zentralen Ort überprüfen können, was Ihnen hilft, Ihre Umgebung zu prüfen und die Einhaltung der Vorschriften nachzuweisen.

Wenn Ihre landing zone Zone-Version älter als 3.0 ist: AWS Config Protokolliert für Ihre registrierten Konten alle Änderungen an Ressourcen für alle Regionen, in denen das Konto betrieben wird. Jede Änderung wird als Configuration Item (CI) modelliert, das Informationen wie die Ressourcen-ID, die

Region, das Datum, an dem jede Änderung aufgezeichnet wurde, und darüber, ob sich die Änderung auf eine bekannte oder eine neu entdeckte Ressource bezieht, enthält.

Wenn Ihre landing zone Zone-Version 3.0 oder höher ist: AWS Control Tower beschränkt die Aufzeichnung für globale Ressourcen wie IAM-Benutzer, Gruppen, Rollen und vom Kunden verwaltete Richtlinien nur auf Ihre Heimatregion. Kopien globaler Ressourcenänderungen werden nicht in jeder Region gespeichert. Diese Beschränkung der Ressourcenaufzeichnung entspricht den AWS Config bewährten Verfahren. Eine vollständige Liste der globalen Ressourcen ist in der AWS Config Dokumentation verfügbar.

- Weitere Informationen dazu finden Sie AWS Config unter So AWS Config funktioniert es.
- Eine Liste der Ressourcen, die unterstützt AWS Config werden können, finden Sie unter Unterstützte Ressourcentypen.
- Weitere Informationen zum Anpassen der Ressourcenverfolgung in der AWS Control Tower-Umgebung finden Sie im Blogbeitrag Customize AWS Config Resource Tracking in AWS Control Tower.

AWS Control Tower richtet für jedes registrierte Konto einen AWS Config Lieferkanal ein. Der Lieferkanal übermittelt aufgezeichnete Änderungen an ein zentrales Konto, wo sie in einem Amazon Simple Storage Service-Bucket AWS Config gespeichert werden. Der Name und der Speicherort des Amazon S3 S3-Buckets hängen von Ihrer landing zone Zone-Version ab:

- Bei landing zone Zone-Version 3.3 oder früher werden die Protokolle im `aws-controltower-logs-*` Amazon S3 S3-Bucket im Protokollarchiv-Konto gespeichert.
- Bei landing zone Zone-Version 4.0 oder höher werden die Protokolle im `aws-controltower-config-logs-*` Amazon S3 S3-Bucket im AWS Config Integrationskonto (früher als Audit-Konto bezeichnet) gespeichert. Weitere Informationen finden Sie unter Aktualisierungen der AWS Config.

Verwalten AWS Config Kosten in AWS Control Tower

In diesem Abschnitt wird beschrieben, wie Änderungen an Ressourcen in Ihren AWS Control Tower Tower-Konten AWS Config aufgezeichnet und Ihnen in Rechnung gestellt werden. Diese Informationen können Ihnen helfen zu verstehen, wie Sie die mit AWS Config der Nutzung von AWS Control Tower verbundenen Kosten verwalten können. Bei AWS Control Tower fallen keine zusätzlichen Kosten an.

> **Note**
>
> Wenn Ihre landing zone Zone-Version 3.0 oder höher ist: AWS Control Tower beschränkt die AWS Config Aufzeichnung für globale Ressourcen wie IAM-Benutzer, Gruppen, Rollen und vom Kunden verwaltete Richtlinien nur auf Ihre Heimatregion. Daher gelten einige der Informationen in diesem Abschnitt möglicherweise nicht für Ihre landing zone.

AWS Config ist so konzipiert, dass jede Änderung an jeder Ressource in jeder Region, in der ein Konto betrieben wird, als Konfigurationselement (CI) aufgezeichnet wird. AWS Config stellt Ihnen jedes Konfigurationselement, das es generiert, in Rechnung.

Wie AWS Config funktioniert

AWS Config zeichnet Ressourcen in jeder Region separat auf. Einige globale Ressourcen, wie z. B. IAM-Rollen, werden einmal pro Region aufgezeichnet. Wenn Sie beispielsweise eine neue IAM-Rolle in einem registrierten Konto erstellen, das in fünf Regionen tätig ist, werden fünf CIs AWS Config generiert, eine für jede Region. Andere globale Ressourcen, wie z. B. Route 53-Hosting-Zonen, werden in allen Regionen nur einmal aufgezeichnet. Wenn Sie beispielsweise eine neue gehostete Route 53-Zone in einem registrierten Konto erstellen, wird unabhängig davon, wie viele Regionen für dieses Konto ausgewählt wurden, ein CI AWS Config generiert. Eine Liste, die Ihnen hilft, diese Ressourcentypen zu unterscheiden, finden Sie unterDieselbe Ressource wird mehrfach aufgezeichnet.

> **Note**
>
> Wenn AWS Control Tower mit arbeitet AWS Config, kann eine Region von AWS Control Tower verwaltet werden oder nicht regiert werden, und die Änderungen werden AWS Config trotzdem aufgezeichnet, wenn das Konto in dieser Region betrieben wird.

AWS Config erkennt zwei Arten von Beziehungen in Ressourcen

AWS Config unterscheidet zwischen direkten und indirekten Beziehungen zwischen Ressourcen. Wenn eine Ressource im Describe-API-Aufruf einer anderen Ressource zurückgegeben wird, werden diese Ressourcen als direkte Beziehung aufgezeichnet. Wenn Sie eine Ressource ändern, die in direkter Beziehung zu einer anderen Ressource AWS Config steht, wird kein CI für beide Ressourcen erstellt.

Wenn Sie beispielsweise eine Amazon EC2 EC2-Instance erstellen und die API verlangt, dass Sie eine Netzwerkschnittstelle erstellen, wird davon ausgegangen, AWS Config dass die Amazon EC2 EC2-Instance eine direkte Beziehung zur Netzwerkschnittstelle hat. AWS Config Generiert daher nur ein CI.

AWS Config zeichnet separate Änderungen für Ressourcenbeziehungen auf, bei denen es sich um indirekte Beziehungen handelt. AWS Config Generiert beispielsweise zwei CIs, wenn Sie eine Sicherheitsgruppe erstellen und eine zugehörige Amazon EC2 EC2-Instance hinzufügen, die Teil der Sicherheitsgruppe ist.

Weitere Informationen zu direkten und indirekten Beziehungen finden Sie unter Was ist eine direkte und eine indirekte Beziehung zu einer Ressource?

Eine Liste der Ressourcenbeziehungen finden Sie in der AWS Config Dokumentation.

Sehen Sie sich die an AWS Config Rekorderdaten zu registrierten Konten

AWS Config ist integriert, CloudWatch sodass Sie AWS Config CIs in einem Dashboard anzeigen können. Weitere Informationen finden Sie im Blogbeitrag AWS Config Unterstützt CloudWatch Amazon-Metriken.

Um AWS Config Daten programmgesteuert anzuzeigen, können Sie mit der AWS CLI arbeiten oder andere AWS Tools verwenden.

Fragen Sie die ab AWS Config Rekorderdaten zu einer bestimmten Ressource

Sie können die AWS CLI verwenden, um eine Liste der letzten Änderungen für eine Ressource abzurufen.

Befehl zum Ressourcenverlauf:

- `aws configservice get-resource-config-history --resource-type RESOURCE-TYPE --resource-id RESOURCE-ID --region REGION`

Weitere Informationen finden Sie in der API-Dokumentation für `get-config-history`.

Visualisieren AWS Config Daten mit Quick

Sie können Ressourcen visualisieren und abfragen, die AWS Config in Ihrem gesamten Unternehmen aufgezeichnet wurden. Weitere Informationen finden Sie im Config Resource Compliance Dashboard und Visualisieren von AWS Config Daten mit Amazon Athena und Quick.

Fehlerbehebung AWS Config im AWS Control Tower

Dieser Abschnitt enthält Informationen zu einigen Problemen, die bei der Verwendung AWS Config mit AWS Control Tower auftreten können.

Hoch AWS Config Kosten

Wenn Ihr Workflow Prozesse umfasst, die häufig Ressourcen erstellen, aktualisieren oder löschen, oder wenn er Ressourcen in großer Anzahl verarbeitet, kann dieser Workflow eine große Anzahl von CIs generieren. Wenn Sie diese Prozesse in einem Konto ausführen, das nicht zur Produktion gehört, sollten Sie erwägen, die Registrierung des Kontos aufzuheben. Möglicherweise müssen Sie den AWS Config Rekorder für dieses Konto manuell deaktivieren.

> **Note**
>
> Nachdem Sie das Konto deregistriert haben, kann AWS Control Tower keine detektivischen Kontrollen erzwingen oder Kontoereignisse wie AWS Config Aktivitäten für Ressourcen in diesem Konto protokollieren.

Weitere Informationen finden Sie unter Verwaltung eines registrierten Kontos aufheben. Informationen zum Deaktivieren des AWS Config Rekorders finden Sie unter Verwaltung des Konfigurationsrekorders.

Dieselbe Ressource wird mehrfach aufgezeichnet

Prüfen Sie, ob es sich bei der Ressource um eine globale Ressource handelt. Für AWS Control Tower Tower-Landezonen vor Version 3.0 AWS Config können bestimmte globale Ressourcen für jede Region, in der sie betrieben AWS Config wird, einmal aufgezeichnet werden. Wenn AWS Config es beispielsweise in acht Regionen aktiviert ist, wird jede Rolle achtmal aufgezeichnet.

Die folgenden Ressourcen werden einmal für jede Region aufgezeichnet, in der AWS Config ist in Betrieb:

- `AWS::IAM::Group`
- `AWS::IAM::Policy`
- `AWS::IAM::Role`
- `AWS::IAM::User`

Andere globale Ressourcen werden nur einmal aufgezeichnet. Hier sind einige Beispiele für Ressourcen, die einmal aufgezeichnet wurden:

- `AWS::Route53::HostedZone`
- `AWS::Route53::HealthCheck`
- `AWS::ECR::PublicRepository`
- `AWS::GlobalAccelerator::Listener`
- `AWS::GlobalAccelerator::EndpointGroup`
- `AWS::GlobalAccelerator::Accelerator`

AWS Config hat keine Ressource aufgezeichnet

Bestimmte Ressourcen haben Abhängigkeitsbeziehungen zu anderen Ressourcen. Diese Beziehungen können direkt oder indirekt sein. Eine Liste der veralteten indirekten Beziehungen finden Sie in den AWS Config häufig gestellten Fragen.

Lebenszyklusereignisse im AWS Control Tower

Bei einigen vom AWS Control Tower protokollierten Ereignissen handelt es sich um Lebenszyklusereignisse. Ein Lebenszyklusereignis dient dazu, den Abschluss bestimmter AWS Control Tower-Aktionen zu markieren, die den Zustand der Ressourcen verändern. Lebenszyklusereignisse beziehen sich auf Ressourcen, die AWS Control Tower erstellt oder verwaltet, z. B. eine Landezone, einen Basiswert oder eine Kontrolle, die sich auf eine Organisationseinheit (OU) oder ein Konto beziehen.

Merkmale von AWS Control Tower-Lebenszyklusereignissen

- Für jedes Lebenszyklusereignis zeigt das Ereignisprotokoll an, ob die ursprüngliche Control Tower-Aktion erfolgreich abgeschlossen wurde oder fehlgeschlagen ist.
- AWS CloudTrail zeichnet jedes Lifecycle-Ereignis automatisch als AWS Nicht-API-Serviceereignis auf. Weitere Informationen finden Sie im AWS CloudTrail Benutzerhandbuch.
- Jedes Lifecycle-Ereignis wird auch an die Amazon EventBridge - und Amazon CloudWatch Events-Dienste übermittelt. Hinweis: Um Lebenszyklus-Ereignisse empfangen zu können EventBridge, benötigen Sie einen aktiven AWS CloudTrail Trail mit aktivierter Protokollierung. Weitere Informationen zu AWS Serviceereignissen, die über bereitgestellt werden AWS CloudTrail,

finden Sie CloudTrail im EventBridge Amazon-Benutzerhandbuch unter AWS-Serviceereignisse, die über AWS bereitgestellt werden.

Lifecycle-Ereignisse im AWS Control Tower bieten zwei Hauptvorteile:

- Da ein Lebenszyklusereignis den Abschluss einer AWS Control Tower-Aktion registriert, können Sie eine EventBridge Amazon-Regel oder eine Amazon CloudWatch Events-Regel erstellen, die je nach Status des Lebenszyklusereignisses die nächsten Schritte in Ihrem Automatisierungsworkflow auslösen kann.
- Die Protokolle bieten zusätzliche Details, um Administratoren und Prüfer bei der Überprüfung bestimmter Aktivitätstypen in Ihren Organisationen zu unterstützen.

Funktionsweise von Lebenszyklusereignissen

AWS Control Tower ist bei der Umsetzung seiner Aktionen auf mehrere Dienste angewiesen. Daher wird jedes Lebenszyklusereignis erst aufgezeichnet, nachdem eine Reihe von Aktionen abgeschlossen ist. Wenn Sie beispielsweise eine Steuerung für eine Organisationseinheit aktivieren, startet AWS Control Tower eine Reihe von Unterschritten, die die Anforderung implementieren. Das Endergebnis der gesamten Reihe von Unterschritten wird im Protokoll als Status des Lebenszyklusereignisses aufgezeichnet.

- Wenn jeder zugrunde liegende Unterschritt erfolgreich abgeschlossen wurde, wird der Lebenszyklusereignis-Status als Succeeded (Erfolgreich) aufgezeichnet.
- Wenn einer der zugrunde liegenden Unterschritte nicht erfolgreich abgeschlossen wurde, wird der Lebenszyklusereignis-Status als Failed (Fehlgeschlagen) aufgezeichnet.

Jedes Lebenszyklusereignis enthält einen protokollierten Zeitstempel, der angibt, wann die AWS Control Tower-Aktion initiiert wurde, und einen weiteren Zeitstempel, der angibt, wann das Lifecycle-Ereignis abgeschlossen ist, was als Erfolg oder Misserfolg kennzeichnet.

Anzeigen von Lebenszyklusereignissen im Control Tower

Sie können Lebenszyklusereignisse auf der Seite Aktivitäten in Ihrem AWS Control Tower-Dashboard einsehen.

- Um zur Seite Activities (Aktivitäten) zu gelangen, wählen Sie im linken Navigationsbereich die Option Activities (Aktivitäten) aus.

- Um weitere Details zu einem bestimmten Ereignis zu erhalten, wählen Sie das Ereignis und dann oben rechts die Schaltfläche View Details (Details anzeigen) aus.

Weitere Informationen zur Integration von AWS Control Tower-Lebenszyklusereignissen in Ihre Workflows finden Sie in diesem Blogbeitrag Using lifecycle events to tracking aws control tower actions and trigger automated workflows.

Erwartetes Verhalten von CreateManagedAccount und UpdateManagedAccount Lebenszyklusereignissen

Wenn Sie ein Konto erstellen oder ein Konto im AWS Control Tower registrieren, rufen diese beiden Aktionen dieselbe interne API auf. Wenn während des Vorgangs ein Fehler auftritt, tritt dieser normalerweise auf, nachdem das Konto erstellt, aber nicht vollständig bereitgestellt wurde. Wenn Sie nach dem Fehler erneut versuchen, das Konto zu erstellen, oder wenn Sie versuchen, das bereitgestellte Produkt zu aktualisieren, erkennt AWS Control Tower, dass das Konto bereits existiert.

Da das Konto existiert, zeichnet AWS Control Tower das `UpdateManagedAccount` Lebenszyklusereignis und nicht das `CreateManagedAccount` Lifecycle-Ereignis am Ende der Wiederholungsanforderung auf. Möglicherweise haben Sie aufgrund des Fehlers mit einem anderen `CreateManagedAccount` Ereignis gerechnet. Das `UpdateManagedAccount` Lebenszyklusereignis ist jedoch das erwartete und gewünschte Verhalten.

Wenn Sie planen, Konten mithilfe automatisierter Methoden bei AWS Control Tower zu erstellen oder zu registrieren, programmieren Sie die Lambda-Funktion so, dass sie sowohl nach UpdateManagedAccount Lebenszyklusereignissen als CreateManagedAccount auch nach Lebenszyklusereignissen sucht.

Namen des Lebenszyklusereignis

Jedes Lebenszyklusereignis ist so benannt, dass es der ursprünglichen Aktion im AWS Control Tower entspricht, die ebenfalls von AWS aufgezeichnet wird. CloudTrail So wird beispielsweise ein Lebenszyklusereignis benannt, das durch das AWS Control `CreateManagedAccount` CloudTrail Tower-Ereignis ausgelöst wurde`CreateManagedAccount`.

Jeder Name in der nachfolgenden Liste ist ein Link zu einem Beispiel der protokollierten Details im `JSON`-Format. Die zusätzlichen Details, die in diesen Beispielen gezeigt werden, stammen aus den CloudWatch Amazon-Ereignisprotokollen.

Obwohl JSON Kommentare nicht unterstützt, wurden zur Erläuterung einige Kommentare in den Beispielen hinzugefügt. Kommentaren wird "//" vorangestellt und sie werden auf der rechten Seite der Beispiele angezeigt.

In diesen Beispielen sind einige Kontonamen und Organisationsnamen verdeckt. Eine `accountId` ist immer eine 12-stellige Zahlenfolge, die in den Beispielen durch "xxxxxxxxxxxx" ersetzt wurde. Eine `organizationalUnitID` ist eine eindeutige Zeichenfolge aus Buchstaben und Zahlen. Ihre Form bleibt in den Beispielen erhalten.

- `CreateManagedAccount`: Das Protokoll zeichnet auf, ob AWS Control Tower jede Aktion zur Erstellung und Bereitstellung eines neuen Kontos mithilfe von Account Factory erfolgreich abgeschlossen hat.
- `UpdateManagedAccount`: Das Protokoll zeichnet auf, ob AWS Control Tower jede Aktion zur Aktualisierung eines bereitgestellten Produkts, das mit einem Konto verknüpft ist, das Sie zuvor mit Account Factory erstellt haben, erfolgreich abgeschlossen hat.
- `EnableGuardrail`: Das Protokoll zeichnet auf, ob AWS Control Tower jede Aktion zur Aktivierung einer Kontrolle für eine Organisationseinheit erfolgreich abgeschlossen hat.
- `DisableGuardrail`: Das Protokoll zeichnet auf, ob AWS Control Tower jede Aktion zur Deaktivierung einer Steuerung auf einer Organisationseinheit erfolgreich abgeschlossen hat.
- `SetupLandingZone`: Das Protokoll zeichnet auf, ob AWS Control Tower jede Aktion zur Einrichtung einer Landezone erfolgreich abgeschlossen hat.
- `UpdateLandingZone`: Das Protokoll zeichnet auf, ob AWS Control Tower jede Aktion zur Aktualisierung Ihrer bestehenden Landezone erfolgreich abgeschlossen hat.
- `RegisterOrganizationalUnit`: Das Protokoll zeichnet auf, ob der AWS Control Tower jede Aktion zur Aktivierung seiner Governance-Funktionen in einer Organisationseinheit erfolgreich abgeschlossen hat.
- `DeregisterOrganizationalUnit`: Das Protokoll zeichnet auf, ob AWS Control Tower jede Aktion zur Deaktivierung seiner Governance-Funktionen in einer OU erfolgreich abgeschlossen hat.
- `PrecheckOrganizationalUnit`: Das Protokoll zeichnet auf, ob AWS Control Tower eine Ressource erkannt hat, die den erfolgreichen Abschluss des Extend Governance-Vorgangs verhindern würde.
- `EnableBaseline`: Im Protokoll wird aufgezeichnet, ob AWS Control Tower jede Aktion zur Aktivierung einer neuen Baseline für ein Zielmitgliedskonto im Rahmen einer OU erfolgreich abgeschlossen hat. Der Aktivierungsvorgang kann mithilfe der `EnableBaseline` API oder der Konsole initiiert werden.

- `ResetEnabledBaseline`: Das Protokoll zeichnet auf, ob AWS Control Tower jede Aktion zum Zurücksetzen einer vorhandenen aktivierten Baseline auf einem Zielmitgliedskonto unter einer OU erfolgreich abgeschlossen hat. Der Reset-Vorgang kann mithilfe der `ResetEnabledBaseline` API oder der Konsole initiiert werden.
- `UpdateEnabledBaseline`: Das Protokoll zeichnet auf, ob AWS Control Tower jede Aktion zur Aktualisierung einer vorhandenen aktivierten Baseline auf einem Zielmitgliedskonto unter einer OU erfolgreich abgeschlossen hat. Der Aktualisierungsvorgang kann über die `UpdateEnabledBaseline` API oder die Konsole initiiert werden.
- `DisableBaseline`: Das Protokoll zeichnet auf, ob AWS Control Tower jede Aktion zur Deaktivierung einer vorhandenen aktivierten Baseline auf einem Zielmitgliedskonto unter einer OU erfolgreich abgeschlossen hat. Der Deaktivierungsvorgang kann über die `DisableBaseline` API oder die Konsole initiiert werden.
- `EnableControl`: Das Protokoll zeichnet auf, ob AWS Control Tower jede Aktion zur Aktivierung einer Kontrolle für ein Zielkonto im Rahmen einer OU erfolgreich abgeschlossen hat. Der Aktivierungsvorgang kann mithilfe der `EnableControl` API oder der Konsole initiiert werden.
- `ResetEnabledControl`: Das Protokoll zeichnet auf, ob AWS Control Tower jede Aktion zum Zurücksetzen einer vorhandenen aktivierten Steuerung auf einem Zielkonto unter einer OU erfolgreich abgeschlossen hat. Der Reset-Vorgang kann über die `ResetEnabledControl` API oder die Konsole initiiert werden.
- `UpdateEnabledControl`: Das Protokoll zeichnet auf, ob AWS Control Tower jede Aktion zur Aktualisierung einer vorhandenen aktivierten Steuerung auf einem Zielkonto unter einer OU erfolgreich abgeschlossen hat. Der Aktualisierungsvorgang kann über die `UpdateEnabledControl` API oder die Konsole initiiert werden.
- `DisableControl`: Das Protokoll zeichnet auf, ob AWS Control Tower jede Aktion zur Deaktivierung einer vorhandenen aktivierten Steuerung für ein Zielkonto unter einer OU erfolgreich abgeschlossen hat. Der Deaktivierungsvorgang kann über die `DisableControl` API oder die Konsole initiiert werden.

Die folgenden Abschnitte enthalten eine Liste der AWS Control Tower-Lebenszyklusereignisse mit Beispielen für die Details, die für jede Art von Lebenszyklusereignis protokolliert wurden.

`CreateManagedAccount`

Dieses Lebenszyklusereignis zeichnet auf, ob AWS Control Tower mithilfe von Account Factory erfolgreich ein neues Konto erstellt und bereitgestellt hat. Dieses Ereignis entspricht dem AWS

Control `CreateManagedAccount` CloudTrail Tower-Ereignis. Das Lebenszyklusereignis-Protokoll enthält den `accountName` und die `accountId` des neu erstellten Kontos und den `organizationalUnitName` und die `organizationalUnitId` der Organisationseinheit, in der sich das Konto befindet.

```
{
    "version": "0",
    "id": "999cccaa-eaaa-0000-1111-123456789012",
    "detail-type": "AWS Service Event via CloudTrail",
    "source": "aws.controltower",
    "account": "XXXXXXXXXXXX",                                    // Management account
 ID.
    "time": "2018-08-30T21:42:18Z",                               // Format: yyyy-MM-
dd'T'hh:mm:ssZ
    "region": "us-east-1",                                        // AWS Control Tower
 home region.
    "resources": [ ],
    "detail": {
        "eventVersion": "1.05",
        "userIdentity": {
            "accountId": "XXXXXXXXXXXX",
            "invokedBy": "AWS Internal"
        },
        "eventTime": "2018-08-30T21:42:18Z",                      // Timestamp when call
 was made. Format: yyyy-MM-dd'T'hh:mm:ssZ.
        "eventSource": "controltower.amazonaws.com",
        "eventName": "CreateManagedAccount",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "AWS Internal",
        "userAgent": "AWS Internal",
        "eventID": "0000000-0000-0000-1111-123456789012",
        "readOnly": false,
        "eventType": "AwsServiceEvent",
        "serviceEventDetails": {
            "createManagedAccountStatus": {
                "organizationalUnit":{
                    "organizationalUnitName":"Custom",
                    "organizationalUnitId":"ou-XXXX-l3zc8b3h"

                    },
                "account":{
                    "accountName":"LifeCycle1",
                    "accountId":"XXXXXXXXXXXX"
```

```
                    },
                "state":"SUCCEEDED",
                "message":"AWS Control Tower successfully created a managed account.",
                "requestedTimestamp":"2019-11-15T11:45:18+0000",
                "completedTimestamp":"2019-11-16T12:09:32+0000"}
        }
    }
}
```

UpdateManagedAccount

Dieses Lebenszyklusereignis zeichnet auf, ob AWS Control Tower das bereitgestellte Produkt, das einem Konto zugeordnet ist, das zuvor mithilfe von Account Factory erstellt wurde, erfolgreich aktualisiert hat. Dieses Ereignis entspricht dem AWS Control `UpdateManagedAccount` CloudTrail Tower-Ereignis. Das Lebenszyklusereignis-Protokoll enthält den `accountName` und die `accountId` des zugeordneten Kontos und den `organizationalUnitName` und die `organizationalUnitId` der Organisationseinheit, in der sich das aktualisierte Konto befindet.

```
{
    "version": "0",
    "id": "999cccaa-eaaa-0000-1111-123456789012",
    "detail-type": "AWS Service Event via CloudTrail",
    "source": "aws.controltower",
    "account": "XXXXXXXXXXXX",                                    // AWS Control Tower
 organization management account.
    "time": "2018-08-30T21:42:18Z",                               // Format: yyyy-MM-
dd'T'hh:mm:ssZ
    "region": "us-east-1",                                        // AWS Control Tower
 home region.
    "resources": [],
    "detail": {
        "eventVersion": "1.05",
        "userIdentity": {
            "accountId": "XXXXXXXXX",
            "invokedBy": "AWS Internal"
        },
        "eventTime": "2018-08-30T21:42:18Z",                      // Timestamp when call
 was made. Format: yyyy-MM-dd'T'hh:mm:ssZ.
        "eventSource": "controltower.amazonaws.com",
        "eventName": "UpdateManagedAccount",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "AWS Internal",
```

```
        "userAgent": "AWS Internal",
        "eventID": "0000000-0000-0000-1111-123456789012",
        "readOnly": false,
        "eventType": "AwsServiceEvent",
        "serviceEventDetails": {
            "updateManagedAccountStatus": {
                "organizationalUnit":{
                    "organizationalUnitName":"Custom",
                    "organizationalUnitId":"ou-XXXX-l3zc8b3h"
                    },
                "account":{
                    "accountName":"LifeCycle1",
                    "accountId":"XXXXXXXXXXXX"
                    },
                "state":"SUCCEEDED",
                "message":"AWS Control Tower successfully updated a managed account.",
                "requestedTimestamp":"2019-11-15T11:45:18+0000",
                "completedTimestamp":"2019-11-16T12:09:32+0000"}
        }
    }
}
```

EnableGuardrail

Dieses Lebenszyklusereignis zeichnet auf, ob AWS Control Tower erfolgreich eine Steuerung für eine Organisationseinheit aktiviert hat, die von AWS Control Tower verwaltet wird. Dieses Ereignis entspricht dem AWS Control `EnableGuardrail` CloudTrail Tower-Ereignis. Das Lebenszyklus-Ereignisprotokoll enthält das `guardrailId` `guardrailBehavior` Ende des Steuerelements `organizationalUnitName` und das Ende `organizationalUnitId` der Organisationseinheit, auf der das Steuerelement aktiviert ist.

```
{
    "version": "0",
    "id": "999cccaa-eaaa-0000-1111-123456789012",
    "detail-type": "AWS Service Event via CloudTrail",
    "source": "aws.controltower",
    "account": "XXXXXXXXXXXX",
    "time": "2018-08-30T21:42:18Z",                                  // End-time of action.
 Format: yyyy-MM-dd'T'hh:mm:ssZ
    "region": "us-east-1",                                           // AWS Control Tower
 home region.
    "resources": [ ],
```

```
    "detail": {
        "eventVersion": "1.05",
        "userIdentity": {
            "accountId": "XXXXXXXXXXXX",
            "invokedBy": "AWS Internal"
        },
        "eventTime": "2018-08-30T21:42:18Z",
        "eventSource": "controltower.amazonaws.com",
        "eventName": "EnableGuardrail",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "AWS Internal",
        "userAgent": "AWS Internal",
        "eventID": "0000000-0000-0000-1111-123456789012",
        "readOnly": false,
        "eventType": "AwsServiceEvent",
        "serviceEventDetails": {
            "enableGuardrailStatus": {
                "organizationalUnits": [
                    {
                      "organizationalUnitName": "Custom",
                      "organizationalUnitId": "ou-vwxy-18vy4yro"
                    }
                  ],
                  "guardrails": [
                    {
                      "guardrailId": "AWS-GR_RDS_INSTANCE_PUBLIC_ACCESS_CHECK",
                      "guardrailBehavior": "DETECTIVE"
                    }
                  ],
                  "state": "SUCCEEDED",
                  "message": "AWS Control Tower successfully enabled a guardrail on an
 organizational unit.",
                  "requestTimestamp": "2019-11-12T09:01:07+0000",
                  "completedTimestamp": "2019-11-12T09:01:54+0000"
                }
        }
    }
}
```


DisableGuardrail

Dieses Lebenszyklusereignis zeichnet auf, ob AWS Control Tower eine Steuerung in einer Organisationseinheit, die von AWS Control Tower verwaltet wird, erfolgreich deaktiviert hat.

Dieses Ereignis entspricht dem AWS Control `DisableGuardrail` CloudTrail Tower-Ereignis. Das Lebenszyklus-Ereignisprotokoll enthält das `guardrailId` `guardrailBehavior` Ende des Steuerelements `organizationalUnitName` und das Ende `organizationalUnitId` der Organisationseinheit, in der das Steuerelement deaktiviert ist.


```
{
    "version": "0",
    "id": "999cccaa-eaaa-0000-1111-123456789012",
    "detail-type": "AWS Service Event via CloudTrail",
    "source": "aws.controltower",
    "account": "XXXXXXXXXXXX",
    "time": "2018-08-30T21:42:18Z",
    "region": "us-east-1",
    "resources": [ ],
    "detail": {
        "eventVersion": "1.05",
        "userIdentity": {
            "accountId": "XXXXXXXXXXXX",
            "invokedBy": "AWS Internal"
        },
        "eventTime": "2018-08-30T21:42:18Z",
        "eventSource": "controltower.amazonaws.com",
        "eventName": "DisableGuardrail",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "AWS Internal",
        "userAgent": "AWS Internal",
        "eventID": "0000000-0000-0000-1111-123456789012",
        "readOnly": false,
        "eventType": "AwsServiceEvent",
        "serviceEventDetails": {
            "disableGuardrailStatus": {
                   "organizationalUnits": [
                    {
                      "organizationalUnitName": "Custom",
                      "organizationalUnitId": "ou-vwxy-18vy4yro"
                    }
                  ],
                  "guardrails": [
                    {
                      "guardrailId": "AWS-GR_RDS_INSTANCE_PUBLIC_ACCESS_CHECK",
                      "guardrailBehavior": "DETECTIVE"
                    }
                  ],
```

```
                "state": "SUCCEEDED",
                "message": "AWS Control Tower successfully disabled a guardrail on an
 organizational unit.",
                "requestTimestamp": "2019-11-12T09:01:07+0000",
                "completedTimestamp": "2019-11-12T09:01:54+0000"
              }
           }
       }
   }
```

SetupLandingZone

Dieses Lebenszyklusereignis zeichnet auf, ob der AWS Control Tower erfolgreich eine Landezone eingerichtet hat. Dieses Ereignis entspricht dem AWS Control `SetupLandingZone` CloudTrail Tower-Ereignis. Das Lebenszyklus-Ereignisprotokoll enthält die `rootOrganizationalId` ID der Organisation, die AWS Control Tower aus dem Verwaltungskonto erstellt. Der Protokolleintrag enthält auch das `organizationalUnitName` und `organizationalUnitId` für jede der Organisationseinheiten sowie das `accountName` und `accountId` für jedes Konto, die erstellt werden, wenn AWS Control Tower die Landezone einrichtet.

```
{
    "version": "0",
    "id": "999cccaa-eaaa-0000-1111-123456789012",                // Request ID.
    "detail-type": "AWS Service Event via CloudTrail",
    "source": "aws.controltower",
    "account": "XXXXXXXXXXXX",                                   // Management account
 ID.
    "time": "2018-08-30T21:42:18Z",                              // Event time from
 CloudTrail.
    "region": "us-east-1",                                       // Management account
 CloudTrail region.
    "resources": [ ],
    "detail": {
        "eventVersion": "1.05",
        "userIdentity": {
            "accountId": "XXXXXXXXXXXX",                         // Management-account
 ID.
            "invokedBy": "AWS Internal"
        },
        "eventTime": "2018-08-30T21:42:18Z",                     // Timestamp when call
 was made. Format: yyyy-MM-dd'T'hh:mm:ssZ.
        "eventSource": "controltower.amazonaws.com",
```

```
       "eventName": "SetupLandingZone",
       "awsRegion": "us-east-1",                                    // AWS Control Tower
home region.
       "sourceIPAddress": "AWS Internal",
       "userAgent": "AWS Internal",
       "eventID": "CloudTrail_event_ID",                            // This value is
generated by CloudTrail.
       "readOnly": false,
       "eventType": "AwsServiceEvent",
       "serviceEventDetails": {
           "setupLandingZoneStatus": {
               "state": "SUCCEEDED",                                 // Status of entire
lifecycle operation.
               "message": "AWS Control Tower successfully set up a new landing zone.",

               "rootOrganizationalId" : "r-1234",
               "organizationalUnits" : [                            // Use a list.
                 {
                   "organizationalUnitName": "Security",             // Security OU
name.
                   "organizationalUnitId": "ou-adpf-302pk332"    // Security OU ID.
                 },
                 {
                   "organizationalUnitName": "Custom",           // Custom OU name.
                   "organizationalUnitId": "ou-adpf-302pk332"    // Custom OU ID.
                 },
               ],
              "accounts": [                                         // All created
accounts are here. Use a list of "account" objects.

                 {
                   "accountName": "Audit",
                   "accountId": "XXXXXXXXXXXX"
                 },
                 {
                   "accountName": "Log archive",
                   "accountId": "XXXXXXXXXXXX"
                 }
             ],
             "requestedTimestamp": "2018-08-30T21:42:18Z",
             "completedTimestamp": "2018-08-30T21:42:18Z"
           }
       }
   }
```

```
}
```

UpdateLandingZone

Dieses Lebenszyklusereignis zeichnet auf, ob der AWS Control Tower Ihre bestehende Landezone erfolgreich aktualisiert hat. Dieses Ereignis entspricht dem AWS Control `UpdateLandingZone` CloudTrail Tower-Ereignis. Das Lebenszyklus-Ereignisprotokoll enthält die `rootOrganizationalId` ID der (aktualisierten) Organisation, die vom AWS Control Tower geleitet wird. Der Protokolleintrag enthält auch das `organizationalUnitName` und `organizationalUnitId` für jede der Organisationseinheiten sowie das `accountName` und `accountId` für jedes Konto, das zuvor bei der ursprünglichen Einrichtung der Landezone durch den AWS Control Tower erstellt wurde.

```
{
    "version": "0",
    "id": "999cccaa-eaaa-0000-1111-123456789012",                // Request ID.
    "detail-type": "AWS Service Event via CloudTrail",
    "source": "aws.controltower",
    "account": "XXXXXXXXXXXX",                                  // Management account
 ID.
    "time": "2018-08-30T21:42:18Z",                             // Event time from
 CloudTrail.
    "region": "us-east-1",                                      // Management account
 CloudTrail region.
    "resources": [ ],
    "detail": {
        "eventVersion": "1.05",
        "userIdentity": {
            "accountId": "XXXXXXXXXXXX",                        // Management account
 ID.
            "invokedBy": "AWS Internal"
        },
        "eventTime": "2018-08-30T21:42:18Z",                    // Timestamp when call
 was made. Format: yyyy-MM-dd'T'hh:mm:ssZ.
        "eventSource": "controltower.amazonaws.com",
        "eventName": "UpdateLandingZone",
        "awsRegion": "us-east-1",                               // AWS Control Tower
 home region.
        "sourceIPAddress": "AWS Internal",
        "userAgent": "AWS Internal",
        "eventID": "CloudTrail_event_ID",                       // This value is
 generated by CloudTrail.
```

```
        "readOnly": false,
        "eventType": "AwsServiceEvent",
        "serviceEventDetails": {
            "updateLandingZoneStatus": {
                "state": "SUCCEEDED",                              // Status of entire
 operation.
                "message": "AWS Control Tower successfully updated a landing zone.",


                "rootOrganizationalId" : "r-1234",
                "organizationalUnits" : [                           // Use a list.
                  {
                    "organizationalUnitName": "Security",             // Security OU
 name.
                    "organizationalUnitId": "ou-adpf-302pk332"    // Security OU ID.
                  },
                  {
                    "organizationalUnitName": "Custom",            // Custom OU name.
                    "organizationalUnitId": "ou-adpf-302pk332"     // Custom OU ID.
                  },
                ],
               "accounts": [                                        // All created
 accounts are here. Use a list of "account" objects.

                  {
                    "accountName": "Audit",
                    "accountId": "XXXXXXXXXXXX"
                  },
                  {
                    "accountName": "Log archive",
                    "accountId": "XXXXXXXXXX"
                  }
              ],
              "requestedTimestamp": "2018-08-30T21:42:18Z",
              "completedTimestamp": "2018-08-30T21:42:18Z"
            }
        }
    }
}
```

RegisterOrganizationalUnit

Dieses Lebenszyklusereignis zeichnet auf, ob der AWS Control Tower seine Governance-Funktionen für eine OU erfolgreich aktiviert hat. Dieses Ereignis entspricht dem AWS Control `RegisterOrganizationalUnit` CloudTrail Tower-Ereignis. Das Lebenszyklus-Ereignisprotokoll enthält das `organizationalUnitName` Ende `organizationalUnitId` der Organisationseinheit, die der AWS Control Tower seiner Verwaltung unterstellt hat.

```
{
    "version": "0",
    "id": "999cccaa-eaaa-0000-1111-123456789012",
    "detail-type": "AWS Service Event via CloudTrail",
    "source": "aws.controltower",
    "account": "123456789012",
    "time": "2018-08-30T21:42:18Z",
    "region": "us-east-1",
    "resources": [ ],
    "detail": {
        "eventVersion": "1.05",
        "userIdentity": {
            "accountId": "XXXXXXXXXXXX",
            "invokedBy": "AWS Internal"
        },
        "eventTime": "2018-08-30T21:42:18Z",
        "eventSource": "controltower.amazonaws.com",
        "eventName": "RegisterOrganizationalUnit",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "AWS Internal",
        "userAgent": "AWS Internal",
        "eventID": "0000000-0000-0000-1111-123456789012",
        "readOnly": false,
        "eventType": "AwsServiceEvent",
        "serviceEventDetails": {
            "registerOrganizationalUnitStatus": {
                "state": "SUCCEEDED",

                "message": "AWS Control Tower successfully registered an organizational
 unit.",

                "organizationalUnit" :
                  {
                    "organizationalUnitName": "Test",
                    "organizationalUnitId": "ou-adpf-302pk332"
```

```
                }
            "requestedTimestamp": "2018-08-30T21:42:18Z",
            "completedTimestamp": "2018-08-30T21:42:18Z"
        }
    }
  }
}
```

DeregisterOrganizationalUnit

Dieses Lebenszyklusereignis zeichnet auf, ob der AWS Control Tower seine Governance-Funktionen in einer Organisationseinheit erfolgreich deaktiviert hat. Dieses Ereignis entspricht dem AWS Control `DeregisterOrganizationalUnit` CloudTrail Tower-Ereignis. Das Lebenszyklus-Ereignisprotokoll enthält das `organizationalUnitName` Ende `organizationalUnitId` der Organisationseinheit, für die der AWS Control Tower seine Governance-Funktionen deaktiviert hat.

```
{
    "version": "0",
    "id": "999cccaa-eaaa-0000-1111-123456789012",
    "detail-type": "AWS Service Event via CloudTrail",
    "source": "aws.controltower",
    "account": "XXXXXXXXXXXX",
    "time": "2018-08-30T21:42:18Z",
    "region": "us-east-1",
    "resources": [ ],
    "detail": {
        "eventVersion": "1.05",
        "userIdentity": {
            "accountId": "XXXXXXXXXXXX",
            "invokedBy": "AWS Internal"
        },
        "eventTime": "2018-08-30T21:42:18Z",
        "eventSource": "controltower.amazonaws.com",
        "eventName": "DeregisterOrganizationalUnit",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "AWS Internal",
        "userAgent": "AWS Internal",
        "eventID": "0000000-0000-0000-1111-123456789012",
        "readOnly": false,
        "eventType": "AwsServiceEvent",
        "serviceEventDetails": {
            "deregisterOrganizationalUnitStatus": {
```

```
                "state": "SUCCEEDED",
                "message": "AWS Control Tower successfully de-registered an
 organizational unit.",
                "organizationalUnit" :
                  {
                    "organizationalUnitName": "Test",                   // Foundational
 OU name.
                    "organizationalUnitId": "ou-adpf-302pk332"          // Foundational
 OU ID.
                  },
                "requestedTimestamp": "2018-08-30T21:42:18Z",
                "completedTimestamp": "2018-08-30T21:42:18Z"
            }
            }
        }
    }
```

PrecheckOrganizationalUnit

Dieses Lebenszyklusereignis zeichnet auf, ob AWS Control Tower erfolgreich Vorprüfungen an einer Organisationseinheit durchgeführt hat. Dieses Ereignis entspricht dem AWS Control `PrecheckOrganizationalUnit` CloudTrail Tower-Ereignis. Das Lebenszyklus-Ereignisprotokoll enthält ein Feld für die `failedPrechecks` Werte `IdName`,, und für jede Ressource, für die AWS Control Tower während des OU-Registrierungsprozesses Vorprüfungen durchgeführt hat.

Das Ereignisprotokoll enthält auch Informationen zu den verschachtelten Konten, für die die Vorprüfungen durchgeführt wurden, einschließlich der Felder `accountNameaccountId`, und. `failedPrechecks`

Wenn der `failedPrechecks` Wert leer ist, bedeutet dies, dass alle Vorabprüfungen für diese Ressource erfolgreich bestanden wurden.

- Dieses Ereignis wird nur ausgelöst, wenn bei der Vorabprüfung ein Fehler auftritt.
- Dieses Ereignis wird nicht ausgelöst, wenn Sie eine leere OU registrieren.

Beispiel für ein Ereignis:

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "accountId": "XXXXXXXXXXXX",
```

```
    "invokedBy": "AWS Internal"
  },
  "eventTime": "2021-09-20T22:45:43Z",
  "eventSource": "controltower.amazonaws.com",
  "eventName": "PrecheckOrganizationalUnit",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "AWS Internal",
  "userAgent": "AWS Internal",
  "eventID": "b41a9d67-0da4-4dc5-a87a-25fa19dc5305",
  "readOnly": false,
  "eventType": "AwsServiceEvent",
  "managementEvent": true,
  "recipientAccountId": "XXXXXXXXXXXX",
  "serviceEventDetails": {
    "precheckOrganizationalUnitStatus": {
      "organizationalUnit": {
        "organizationalUnitName": "Ou-123",
        "organizationalUnitId": "ou-abcd-123456",
        "failedPrechecks": [
            "SCP_CONFLICT"
          ]
      },
      "accounts": [
        {
          "accountName": "Child Account 1",
          "accountId": "XXXXXXXXXXXX",
          "failedPrechecks": [
            "FAILED_TO_ASSUME_ROLE"
          ]
        },
        {
          "accountName": "Child Account 2",
          "accountId": "XXXXXXXXXXXX",
          "failedPrechecks": [
            "FAILED_TO_ASSUME_ROLE"
          ]
        },
        {
          "accountName": "Management Account",
          "accountId": "XXXXXXXXXXXX",
          "failedPrechecks": [
            "MISSING_PERMISSIONS_AF_PRODUCT"
          ]
        },
```

```
        {
          "accountName": "Child Account 3",
          "accountId": "XXXXXXXXXXXX",
          "failedPrechecks": []
        },
        ...
      ],
      "state": "FAILED",
      "message": "AWS Control Tower failed to register an organizational unit due to
 pre-check failures. Go to the OU details page to download a list of failed pre-checks
 for the OU and accounts within.",
      "requestedTimestamp": "2021-09-20T22:44:02+0000",
      "completedTimestamp": "2021-09-20T22:45:43+0000"
    }
  },
  "eventCategory": "Management"
}
```

EnableBaseline

Dieses Lebenszyklusereignis zeichnet auf, ob AWS Control Tower erfolgreich eine Baseline für ein Zielmitgliedskonto im Rahmen einer OU aktiviert hat. Dieses Ereignis entspricht dem `RegisterOrganizationalUnit` oder den `EnableBaseline` CloudTrail Ereignissen im AWS Control Tower. Das Lebenszyklus-Ereignisprotokoll enthält die Baseline, die aktiviert wurde, und ihre Version, die, `targetIdentifier` auf der die Baseline aktiviert wurde, die Baseline, die auf `parentIdentifier` der übergeordneten OU aktiviert wurde, und die `statusSummary` Anzeige des Status SUCCEED oder FAILED sowie die zusätzlichen Parameter und den Zeitstempel des Vorgangs.

```
{
    "eventVersion": "1.11",
    "userIdentity": {
        "accountId": "XXXXXXXXXXXX",
        "invokedBy": "AWS Internal"
    },
    "eventTime": "2025-02-10T17:14:57Z",
    "eventSource": "controltower.amazonaws.com",
    "eventName": "EnableBaseline",
    "awsRegion": "us-east-2",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "AWS Internal",
    "requestParameters": null,
```

```
    "responseElements": null,
    "eventID": "366911a2-4fa6-4e4a-ac2b-280f627e0027",
    "readOnly": false,
    "eventType": "AwsServiceEvent",
    "managementEvent": true,
    "recipientAccountId": "XXXXXXXXXXXX",
    "serviceEventDetails": {
        "enableBaselineStatus": {
            "enabledBaselineDetails": {
                "arn": "arn:aws:controltower:us-east-2:XXXXXXXXXXXX:enabledbaseline/
XXXXXXXXXXXXXXXX",
                "parentIdentifier": "arn:aws:controltower:us-
east-2:XXXXXXXXXXXX:enabledbaseline/XXXXXXXXXXXXXXXX",
                "targetIdentifier": "arn:aws:organizations::XXXXXXXXXXXX:account/o-
ern76xmzvf/XXXXXXXXXXXX",
                "baselineIdentifier": "arn:aws:controltower:us-east-2::baseline/
XXXXXXXXXXXXXXX",
                "baselineVersion": "4.0",
                "statusSummary": {
                    "lastOperationIdentifier": "37f5eb68-e5b9-4c70-ae76-4ca15f6b16de",
                    "status": "SUCCEEDED"
                },
                "parameters": [
                    {
                        "key": "IdentityCenterEnabledBaselineArn",
                        "value": {
                            "untyped": {
                                "object": "arn:aws:controltower:us-
east-2:XXXXXXXXXXXX:enabledbaseline/XXXXXXXXXXXXXXXX"                            }
                        }
                    }
                ]
            },
            "requestedTimestamp": "2025-02-10T17:07:09+0000",
            "completedTimestamp": "2025-02-10T17:14:57+0000"
        }
    },
    "eventCategory": "Management"
}
```

ResetEnabledBaseline

Dieses Lebenszyklusereignis zeichnet auf, ob AWS Control Tower die bestehende aktivierte Baseline auf einem Zielmitgliedskonto unter einer OU erfolgreich zurückgesetzt hat. Dieses Ereignis entspricht dem `RegisterOrganizationalUnit` oder den `ResetEnabledBaseline` CloudTrail Ereignissen im AWS Control Tower. Das Lebenszyklus-Ereignisprotokoll enthält die Baseline, die aktiviert wurde, und ihre Version, die, `targetIdentifier` auf der die Baseline aktiviert wurde, die Baseline, die auf `parentIdentifier` der übergeordneten OU aktiviert wurde, und die `statusSummary` Anzeige des Status SUCCEED oder FAILED sowie die zusätzlichen Parameter und den Zeitstempel des Vorgangs.


```
{
    "eventVersion": "1.11",
    "userIdentity": {
        "accountId": "XXXXXXXXXXXX",
        "invokedBy": "AWS Internal"
    },
    "eventTime": "2025-02-10T21:17:55Z",
    "eventSource": "controltower.amazonaws.com",
    "eventName": "ResetEnabledBaseline",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "AWS Internal",
    "requestParameters": null,
    "responseElements": null,
    "eventID": "c01a32e1-13ab-4b46-8f1b-00699ef6f989",
    "readOnly": false,
    "eventType": "AwsServiceEvent",
    "managementEvent": true,
    "recipientAccountId": "XXXXXXXXXXXX",
    "serviceEventDetails": {
        "resetEnabledBaselineStatus": {
            "enabledBaselineDetails": {
                "arn": "arn:aws:controltower:us-west-2:XXXXXXXXXXXX:enabledbaseline/
XXXXXXXXXXXXXXXX",
                "parentIdentifier": "arn:aws:controltower:us-
west-2:XXXXXXXXXXXX:enabledbaseline/XXXXXXXXXXXXXXXX",
                "targetIdentifier": "arn:aws:organizations::XXXXXXXXXXXX:account/
o-0uh2kplf6d/XXXXXXXXXXXX",
                "baselineIdentifier": "arn:aws:controltower:us-west-2::baseline/
XXXXXXXXXXXXXXX",
                "baselineVersion": "1.0",
```

```
                "statusSummary": {
                    "lastOperationIdentifier": "3e364c89-89fa-42b8-9776-9f7cc47ba1fa",
                    "status": "SUCCEEDED"
                },
                "parameters": []
            },
            "requestedTimestamp": "2025-02-10T21:14:24Z",
            "completedTimestamp": "2025-02-10T21:17:54+0000"
        }
    },
    "eventCategory": "Management"
}
```

UpdateEnabledBaseline

Dieses Lebenszyklusereignis zeichnet auf, ob AWS Control Tower die bestehende aktivierte Baseline auf einem Zielmitgliedskonto unter einer OU erfolgreich aktualisiert hat. Dieses Ereignis entspricht dem `RegisterOrganizationalUnit` oder den `UpdateEnabledBaseline` CloudTrail Ereignissen im AWS Control Tower. Das Lebenszyklus-Ereignisprotokoll enthält die Baseline, die aktiviert wurde, und ihre Version, die, `targetIdentifier` auf der die Baseline aktiviert wurde, die Baseline, die auf `parentIdentifier` der übergeordneten OU aktiviert wurde, und die `statusSummary` Anzeige des Status SUCCEED oder FAILED sowie die zusätzlichen Parameter und den Zeitstempel des Vorgangs.

```
{
    "eventVersion": "1.11",
    "userIdentity": {
        "accountId": "XXXXXXXXXXXX",
        "invokedBy": "AWS Internal"
    },
    "eventTime": "2025-02-10T19:45:28Z",
    "eventSource": "controltower.amazonaws.com",
    "eventName": "UpdateEnabledBaseline",
    "awsRegion": "us-east-2",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "AWS Internal",
    "requestParameters": null,
    "responseElements": null,
    "eventID": "514f2aff-1a99-4912-bda1-0d4d6662c96e",
    "readOnly": false,
    "eventType": "AwsServiceEvent",
    "managementEvent": true,
```

```
    "recipientAccountId": "XXXXXXXXXXXX",
    "serviceEventDetails": {
        "updateEnabledBaselineStatus": {
            "enabledBaselineDetails": {
                "arn": "arn:aws:controltower:us-east-2:XXXXXXXXXXXX:enabledbaseline/
XXXXXXXXXXXXXXXX",
                "parentIdentifier": "arn:aws:controltower:us-
east-2:XXXXXXXXXXXX:enabledbaseline/XXXXXXXXXXXXXXXX",
                "targetIdentifier": "arn:aws:organizations::XXXXXXXXXXXX:account/o-
ern76xmzvf/XXXXXXXXXXXX",
                "baselineIdentifier": "arn:aws:controltower:us-east-2::baseline/
XXXXXXXXXXXXXXX",
                "baselineVersion": "4.0",
                "statusSummary": {
                    "lastOperationIdentifier": "ba3de28f-83fb-4c9a-8a8c-a4e15fac2c41",
                    "status": "SUCCEEDED"
                },
                "parameters": [
                    {
                        "key": "IdentityCenterEnabledBaselineArn",
                        "value": {
                            "untyped": {
                                "object": "arn:aws:controltower:us-
east-2:XXXXXXXXXXXX:enabledbaseline/XXXXXXXXXXXXXXXX"                            }
                        }
                    }
                ]
            },
            "requestedTimestamp": "2025-02-10T19:39:35+0000",
            "completedTimestamp": "2025-02-10T19:45:28+0000"
        }
    },
    "eventCategory": "Management"
}
```


DisableBaseline

Dieses Lebenszyklusereignis zeichnet auf, ob AWS Control Tower die bestehende aktivierte Baseline auf einem Zielmitgliedskonto unter einer OU erfolgreich deaktiviert hat. Dieses Ereignis entspricht dem AWS Control `DisableBaseline` CloudTrail Tower-Ereignis. Das Lebenszyklus-Ereignisprotokoll enthält die Baseline, die aktiviert wurde, und ihre Version, die, `targetIdentifier` auf der die Baseline aktiviert wurde, die Baseline, die auf `parentIdentifier` der übergeordneten

OU aktiviert wurde, und die `statusSummary` Anzeige des Status SUCCEED oder FAILED sowie die zusätzlichen Parameter und den Zeitstempel des Vorgangs.


```
{
    "eventVersion": "1.11",
    "userIdentity": {
        "accountId": "XXXXXXXXXXXX",
        "invokedBy": "AWS Internal"
    },
    "eventTime": "2025-03-14T00:50:58Z",
    "eventSource": "controltower.amazonaws.com",
    "eventName": "DisableBaseline",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "AWS Internal",
    "requestParameters": null,
    "responseElements": null,
    "eventID": "704794c4-a32e-4960-8386-c7efaa5a22a1",
    "readOnly": false,
    "eventType": "AwsServiceEvent",
    "managementEvent": true,
    "recipientAccountId": "XXXXXXXXXXXX",
    "serviceEventDetails": {
        "disableBaselineStatus": {
            "enabledBaselineDetails": {
                "arn": "arn:aws:controltower:us-west-2:XXXXXXXXXXXX:enabledbaseline/
XXXXXXXXXXXXXXXX",
                "parentIdentifier": "arn:aws:controltower:us-
west-2:XXXXXXXXXXXX:enabledbaseline/XXXXXXXXXXXXXXXX",
                "targetIdentifier": "arn:aws:organizations::XXXXXXXXXXXX:account/
o-0uh2kplf6d/XXXXXXXXXXXX",
                "baselineIdentifier": "arn:aws:controltower:us-west-2::baseline/
XXXXXXXXXXXXXXX",
                "baselineVersion": "1.0",
                "statusSummary": {
                    "lastOperationIdentifier": "7b895594-0edb-48bc-9f3d-d88c2ad618df",
                    "status": "SUCCEEDED"
                },
                "parameters": []
            },
            "baselineDetails": {
                "arn": "arn:aws:controltower:us-west-2:XXXXXXXXXXXX:enabledbaseline/
XXXXXXXXXXXXXXXX",
```

```
                "parentIdentifier": "arn:aws:controltower:us-
west-2:XXXXXXXXXXXX:enabledbaseline/XXXXXXXXXXXXXXXX",
                "targetIdentifier": "arn:aws:organizations::XXXXXXXXXXXX:account/
o-0uh2kplf6d/XXXXXXXXXXXX",
                "baselineIdentifier": "arn:aws:controltower:us-west-2::baseline/
XXXXXXXXXXXXXXX",
                "baselineVersion": "1.0",
                "statusSummary": {
                    "lastOperationIdentifier": "7b895594-0edb-48bc-9f3d-d88c2ad618df",
                    "status": "SUCCEEDED"
                },
                "parameters": []
            },
            "requestedTimestamp": "2025-03-14T00:49:13Z",
            "completedTimestamp": "2025-03-14T00:50:58+0000"
        }
    },
    "eventCategory": "Management"
}
```

EnableControl

Dieses Lebenszyklusereignis zeichnet auf, ob AWS Control Tower erfolgreich eine Kontrolle für ein Zielkonto aktiviert hat, das von AWS Control Tower verwaltet wird. Dieses Ereignis entspricht dem AWS Control `EnableControl` CloudTrail Tower-Ereignis und wird ausgelöst, wenn eine Steuerung über die `EnableControl` API oder die Konsole aktiviert wird. Das Lebenszyklus-Ereignisprotokoll enthält Informationen über das aktivierte Steuerelement, das `arn` daraufhin aktivierte Steuerelement, das aktivierte Steuerelement auf `parentIdentifier` der übergeordneten Organisationseinheit, das Steuerelement, `targetIdentifier` auf dem das Steuerelement aktiviert wurde, und die `state` Anzeige des Status SUCCEED oder FAILED `message` sowie die Zeitstempel des Vorgangs. `controlIdentifier`

> **Note**
>
> Das `EnableControl` Lebenszyklusereignis entspricht der `EnableControl` API. AWS Control Tower gibt auch das `EnableGuardrail` Legacy-Lifecycle-Ereignis aus, wenn ein Steuerelement aktiviert wird. Wenn Sie eine Automatisierung erstellen, die auf die Aktivierung von Steuerelementen reagiert, berücksichtigen Sie beide Ereignisnamen.

```
{
    "eventVersion": "1.11",
    "userIdentity": {
        "accountId": "XXXXXXXXXXXX",
        "invokedBy": "AWS Internal"
    },
    "eventTime": "2026-01-07T15:59:28Z",
    "eventSource": "controltower.amazonaws.com",
    "eventName": "EnableControl",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "AWS Internal",
    "requestParameters": null,
    "responseElements": null,
    "eventID": "a4f45d0d-ab6d-41c7-9f97-786d80ff23d2",
    "readOnly": false,
    "eventType": "AwsServiceEvent",
    "managementEvent": true,
    "recipientAccountId": "XXXXXXXXXXXX",
    "serviceEventDetails": {
        "enableControlStatus": {
            "arn": "arn:aws:controltower:us-
east-1:XXXXXXXXXXXX:enabledcontrol/143RH67Q683RJ20V",
            "parentIdentifier": "arn:aws:controltower:us-
east-1:XXXXXXXXXXXX:enabledcontrol/8WU3TCOLC0JPSV6T",
            "controlIdentifier": "arn:aws:controltower:us-east-1::control/AWS-
GR_AUDIT_BUCKET_LOGGING_ENABLED",
            "targetIdentifier": "arn:aws:organizations::XXXXXXXXXXXX:account/o-
k54j7iydcs/XXXXXXXXXXXX",
            "state": "SUCCEEDED",
            "message": "AWS Control Tower successfully enabled a control on the
 target.",
            "requestedTimestamp": "2026-01-07T15:59:24+0000",
            "completedTimestamp": "2026-01-07T15:59:28+0000"
        }
    },
    "eventCategory": "Management"
}
```

ResetEnabledControl

Dieses Lebenszyklusereignis zeichnet auf, ob der AWS Control Tower ein vorhandenes aktiviertes Steuerelement auf einem Zielkonto, das von AWS Control Tower verwaltet wird, erfolgreich zurückgesetzt hat. Dieses Ereignis entspricht dem AWS Control `ResetEnabledControl` CloudTrail Tower-Ereignis und wird ausgelöst, wenn ein aktiviertes Steuerelement mithilfe der `ResetEnabledControl` API oder der Konsole zurückgesetzt wird. Das Lifecycle-Ereignisprotokoll enthält die Daten `controlIdentifier` des Steuerelements, `arn` des aktivierten Steuerelements, das `parentIdentifier` des aktivierten Steuerelements auf der übergeordneten OU, das Steuerelement, `targetIdentifier` auf dem das Steuerelement zurückgesetzt wurde, und die `state` Anzeige des Status SUCCEED oder FAILED sowie a `message` und die Zeitstempel des Vorgangs.


```
{
    "eventVersion": "1.11",
    "userIdentity": {
        "accountId": "XXXXXXXXXXXX",
        "invokedBy": "AWS Internal"
    },
    "eventTime": "2026-01-07T16:10:42Z",
    "eventSource": "controltower.amazonaws.com",
    "eventName": "ResetEnabledControl",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "AWS Internal",
    "requestParameters": null,
    "responseElements": null,
    "eventID": "c82d6f3a-4b9e-43ca-8d21-1a3f8d5b62e9",
    "readOnly": false,
    "eventType": "AwsServiceEvent",
    "managementEvent": true,
    "recipientAccountId": "XXXXXXXXXXXX",
    "serviceEventDetails": {
        "resetEnabledControlStatus": {
            "arn": "arn:aws:controltower:us-
east-1:XXXXXXXXXXXX:enabledcontrol/143RH67Q683RJ20V",
            "parentIdentifier": "arn:aws:controltower:us-
east-1:XXXXXXXXXXXX:enabledcontrol/8WU3TCOLC0JPSV6T",
            "controlIdentifier": "arn:aws:controltower:us-east-1::control/AWS-
GR_AUDIT_BUCKET_LOGGING_ENABLED",
```

```
            "targetIdentifier": "arn:aws:organizations::XXXXXXXXXXXX:account/o-
k54j7iydcs/XXXXXXXXXXXX",
            "state": "SUCCEEDED",
            "message": "AWS Control Tower has successfully reset the enabled control on
 the target.",
            "requestedTimestamp": "2026-01-07T16:10:36+0000",
            "completedTimestamp": "2026-01-07T16:10:42+0000"
        }
    },
    "eventCategory": "Management"
}
```

UpdateEnabledControl

Dieses Lebenszyklusereignis zeichnet auf, ob AWS Control Tower ein vorhandenes aktiviertes Steuerelement auf einem Zielkonto, das von AWS Control Tower verwaltet wird, erfolgreich aktualisiert hat. Dieses Ereignis entspricht dem AWS Control `UpdateEnabledControl` CloudTrail Tower-Ereignis und wird ausgelöst, wenn ein aktiviertes Steuerelement mithilfe der `UpdateEnabledControl` API oder der Konsole aktualisiert wird. Das Lifecycle-Ereignisprotokoll enthält die Daten `controlIdentifier` des Steuerelements, `arn` des aktivierten Steuerelements, das `parentIdentifier` des aktivierten Steuerelements auf der übergeordneten OU, das Steuerelement, `targetIdentifier` auf dem das Steuerelement aktualisiert wurde, und die `state` Anzeige des Status SUCCEED oder FAILED sowie a `message` und die Zeitstempel des Vorgangs.

```
{
    "eventVersion": "1.11",
    "userIdentity": {
        "accountId": "XXXXXXXXXXXX",
        "invokedBy": "AWS Internal"
    },
    "eventTime": "2026-01-07T16:25:19Z",
    "eventSource": "controltower.amazonaws.com",
    "eventName": "UpdateEnabledControl",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "AWS Internal",
    "requestParameters": null,
    "responseElements": null,
    "eventID": "d93e7a4b-5caf-44db-9e32-2b4a9e6c73fa",
    "readOnly": false,
    "eventType": "AwsServiceEvent",
```

```
    "managementEvent": true,
    "recipientAccountId": "XXXXXXXXXXXX",
    "serviceEventDetails": {
        "updateEnabledControlStatus": {
            "arn": "arn:aws:controltower:us-
east-1:XXXXXXXXXXXX:enabledcontrol/143RH67Q683RJ20V",
            "parentIdentifier": "arn:aws:controltower:us-
east-1:XXXXXXXXXXXX:enabledcontrol/8WU3TCOLC0JPSV6T",
            "controlIdentifier": "arn:aws:controltower:us-east-1::control/AWS-
GR_AUDIT_BUCKET_LOGGING_ENABLED",
            "targetIdentifier": "arn:aws:organizations::XXXXXXXXXXXX:account/o-
k54j7iydcs/XXXXXXXXXXXX",
            "state": "SUCCEEDED",
            "message": "AWS Control Tower successfully updated the enabled control on
 the target.",
            "requestedTimestamp": "2026-01-07T16:25:13+0000",
            "completedTimestamp": "2026-01-07T16:25:19+0000"
        }
    },
    "eventCategory": "Management"
}
```


`DisableControl`

Dieses Lebenszyklusereignis zeichnet auf, ob AWS Control Tower ein vorhandenes aktiviertes Steuerelement auf einem Zielkonto, das von AWS Control Tower verwaltet wird, erfolgreich deaktiviert hat. Dieses Ereignis entspricht dem AWS Control `DisableControl` CloudTrail Tower-Ereignis und wird ausgelöst, wenn eine Steuerung über die `DisableControl` API oder die Konsole deaktiviert wird. Das Lifecycle-Ereignisprotokoll enthält die Daten `controlIdentifier` des Steuerelements, `arn` des aktivierten Steuerelements, das `parentIdentifier` des aktivierten Steuerelements auf der übergeordneten OU, das Steuerelement, `targetIdentifier` auf dem das Steuerelement deaktiviert wurde, und die `state` Anzeige des Status SUCCEED oder FAILED `message` sowie die Zeitstempel des Vorgangs.

> **Note**
>
> AWS Control Tower gibt auch das `DisableGuardrail` Legacy-Lifecycle-Ereignis aus, wenn ein Steuerelement deaktiviert wird. Wenn Sie eine Automatisierung erstellen, die auf die Deaktivierung von Steuerelementen reagiert, berücksichtigen Sie beide Ereignisnamen.

```
{
    "eventVersion": "1.11",
    "userIdentity": {
        "accountId": "XXXXXXXXXXXX",
        "invokedBy": "AWS Internal"
    },
    "eventTime": "2026-01-07T16:42:11Z",
    "eventSource": "controltower.amazonaws.com",
    "eventName": "DisableControl",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "AWS Internal",
    "requestParameters": null,
    "responseElements": null,
    "eventID": "e04f8b5c-6dba-45ec-af43-3c5b0f7d84ab",
    "readOnly": false,
    "eventType": "AwsServiceEvent",
    "managementEvent": true,
    "recipientAccountId": "XXXXXXXXXXXX",
    "serviceEventDetails": {
        "disableControlStatus": {
            "arn": "arn:aws:controltower:us-
east-1:XXXXXXXXXXXX:enabledcontrol/143RH67Q683RJ20V",
            "parentIdentifier": "arn:aws:controltower:us-
east-1:XXXXXXXXXXXX:enabledcontrol/8WU3TCOLC0JPSV6T",
            "controlIdentifier": "arn:aws:controltower:us-east-1::control/AWS-
GR_AUDIT_BUCKET_LOGGING_ENABLED",
            "targetIdentifier": "arn:aws:organizations::XXXXXXXXXXXX:account/o-
k54j7iydcs/XXXXXXXXXXXX",
            "state": "SUCCEEDED",
            "message": "AWS Control Tower successfully disabled the enabled control on
 the target.",
            "requestedTimestamp": "2026-01-07T16:42:05+0000",
            "completedTimestamp": "2026-01-07T16:42:11+0000"
        }
    },
    "eventCategory": "Management"
}
```

Verwenden AWS Benutzerbenachrichtigungen mit AWS Control Tower

Sie können AWS Benutzerbenachrichtigungen verwenden, um Zustellungskanäle einzurichten, über die Sie über AWS Control Tower Ereignisse informiert werden können. Sie erhalten eine Benachrichtigung, wenn ein Ereignis einer von Ihnen angegebenen Regel entspricht. Sie können Benachrichtigungen für Ereignisse über mehrere Kanäle erhalten, darunter E-Mail, Chat-Benachrichtigungen von Amazon Q Developer in Chat-Anwendungen oder Push-Benachrichtigungen für die mobile AWS Konsolen-App. Benachrichtigungen werden auch im Console Notifications Center angezeigt.

AWS Benutzerbenachrichtigungen unterstützen die Aggregation, wodurch die Anzahl der Benachrichtigungen, die Sie bei bestimmten Ereignissen erhalten, reduziert werden kann. Benachrichtigungen sind auch im Benachrichtigungscenter der Konsole sichtbar.

Das Abonnieren von Benachrichtigungen über AWS Benutzerbenachrichtigungen anstatt über EventBridge folgende Vorteile bietet:

- Eine benutzerfreundlichere Benutzeroberfläche (UI).
- Integration mit der AWS Konsole im bell/notifications Bereich der globalen Navigationsleiste.
- Native Unterstützung für E-Mail-Benachrichtigungen, Amazon SNS muss nicht eingerichtet werden.
- Vor allem Unterstützung für mobile Push-Benachrichtigungen, exklusiv für AWS Benutzerbenachrichtigungen.

Eine Art von Benachrichtigung, die Sie möglicherweise erhalten möchten, ist beispielsweise der Fall, dass Security Hub CSPM kritische und schwerwiegende Ergebnisse enthält. Ein JSON-Codeausschnitt zum Einrichten dieses Benachrichtigungsabonnements könnte etwa so aussehen:

```
{
  "detail": {
    "findings": {
      "Compliance": {
        "Status": ["FAILED", "WARNING", "NOT_AVAILABLE"]
      },
      "RecordState": ["ACTIVE"],
      "Severity": {
        "Label": ["CRITICAL", "HIGH"]
      },
```

```
      "Workflow": {
        "Status": ["NEW", "NOTIFIED"]
      }
    }
  }
}
```

Filterung von Ereignissen

- Sie können Ereignisse mithilfe der in der AWS Benutzerbenachrichtigungskonsole verfügbaren Filter nach Dienst und Namen filtern.
- Sie können Ereignisse nach bestimmten Eigenschaften filtern, wenn Sie Ihren eigenen EventBridge Filter aus JSON-Code erstellen.

Beispiel für ein AWS Control Tower Ereignis

Hier ist ein verallgemeinertes Beispielereignis für AWS Control Tower.

- Es ist ein EventBridge Ereignis.
- Sie können EventBridge Ereignisse (wie dieses) mithilfe von AWS Benutzerbenachrichtigungen abonnieren.

```
{
    "version": "0",
    "id": "<id>", // alphanumeric string
    "detail-type": "AWS Service Event via CloudTrail",
    "source": "aws.controltower",
    "account": "<account ID>", // Management account ID.
    "time": "<date>", // Format: yyyy-MM-dd'T'hh:mm:ssZ
    "region": "<region>", // AWS Control Tower home region.
    "resources": [],
    "detail": {
        "eventVersion": "1.05",
        "userIdentity": {
            "accountId": "121212121212",
            "invokedBy": "AWS Internal"
        },
        "eventTime": "2018-08-30T21:42:18Z", // Timestamp when call was made. Format:
 yyyy-MM-dd'T'hh:mm:ssZ.
        "eventSource": "controltower.amazonaws.com",
```

```
        "eventName": "<event name>", // one of the event names listed in https://
docs.aws.amazon.com/controltower/latest/userguide/lifecycle-events.html
        "awsRegion": "<region>",
        "sourceIPAddress": "AWS Internal",
        "userAgent": "AWS Internal",
        "eventID": "<id>",
        "readOnly": false,
        "eventType": "AwsServiceEvent",
        "serviceEventDetails": {
            // the contents of this object vary depending on the event subtype and
 event state
        }
    }
}
```

AWS Backup und AWS Control Tower

AWS Backup ist ein Dienst, mit dem Sie Pläne für die automatische Sicherung Ihrer AWS Ressourcen erstellen können. Um Backups für Ihre AWS Control Tower Tower-Ressourcen einzurichten, müssen Sie vier Hauptschritte befolgen:

1. Aktiviere es AWS Backup für deine landing zone. Sie können dies auf der Seite mit den Landingzone-Einstellungen in der AWS Control Tower Tower-Konsole tun. Wenn Sie die Option aktivieren AWS Backup, werden Ressourcen in mehreren Konten erstellt. Weitere Informationen finden Sie unter Ressourcen erstellt für AWS Backup.
2. Opt-in zu Backups für AWS Control Tower in der AWS Backup Konsole. Weitere Informationen finden Sie im AWS Backup Entwicklerhandbuch unter Arbeiten mit unterstützten Services.
3. AWS Backup Aktivieren Sie die Option für die einzelnen Organisationseinheiten, die Sie einbeziehen möchten. Sie können diese Aufgabe auf der Seite mit den OU-Details in der Konsole ausführen, nachdem Sie sie auf AWS Backup Landingzone-Ebene aktiviert haben. Wenn Sie die Aktivierung AWS Backup auf einer Organisationseinheit durchführen, erhalten die Konten in dieser Organisationseinheit lokale AWS Backup Tresore.
4. Kennzeichnen Sie die ausgewählten Ressourcen, die in die Backups aufgenommen werden sollen. Das Tag gibt die Häufigkeit der Backups für diese Ressource an. Ihr Backup-Plan folgt dem Zeitplan, der in den Ressourcen-Tags für jede Ressource angegeben ist.

Weitere Informationen finden Sie im AWS Backup Entwicklerhandbuch. Bei der Konfiguration von AWS Backup mit AWS Control Tower fallen keine Kosten an. Es fallen Kosten an von AWS Backup. Informationen zu Preisen finden Sie unter AWS Backup -Preise.

Weitere Informationen zu den AWS Backup Ressourcen, die AWS Control Tower in Ihrer AWS Control Tower Tower-Landezone erstellt, finden Sie unter Ressourcen erstellt für AWS Backup

> **Note**
>
> AWS Control Tower unterstützt die Einrichtung von Backup-Plänen für AWS Control Tower Tower-Ressourcen nicht direkt über den AWS Backup Service, ohne ihn auch im AWS Control Tower Tower-Service zu aktivieren.

Voraussetzungen

Bevor Sie Ihre AWS Control Tower Tower-Ressourcen einrichten AWS Backup können, müssen Sie über eine bestehende AWS Organizations Organisation verfügen. Wenn Sie Ihre AWS Control Tower Tower-Landezone bereits eingerichtet haben, dient diese als Ihre bestehende Organisation.

Sie müssen zwei weitere AWS Konten zuweisen oder erstellen, die nicht bei AWS Control Tower registriert sind. Diese Konten werden zum zentralen Backup-Konto und zum Backup-Administratorkonto. Benennen Sie diese Konten mit diesen Namen.

Außerdem müssen Sie einen Multi-Region-Schlüssel AWS Key Management Service (KMS) speziell für AWS Backup auswählen oder erstellen.

Definieren Sie Ihre Voraussetzungen

- Das zentrale Backup-Konto — Das zentrale Backup-Konto speichert Ihren AWS Control Tower-Backup-Tresor und Ihre Backups. Dieser Tresor wird in allen Bereichen erstellt AWS-Regionen , die von AWS Control Tower verwaltet werden, innerhalb dieses Kontos. Cross-account Kopien werden in diesem Konto gespeichert, falls ein Konto kompromittiert wurde und eine Datenwiederherstellung erforderlich ist.
- Das Backup-Administratorkonto — Das Backup-Administratorkonto ist das delegierte Administratorkonto für den AWS Backup Service in AWS Control Tower. Es speichert die Backup Audit Manager (BAM) -Berichtspläne. Dieses Konto fasst alle Backup-Überwachungsdaten zusammen, z. B. Wiederherstellungsaufträge und Kopieraufträge. Die Daten werden in einem Amazon S3 S3-Bucket gespeichert. Weitere Informationen finden Sie im AWS Backup Entwicklerhandbuch unter Erstellen von Berichtsplänen mithilfe der AWS Backup Konsole.
- Richtlinienanforderung für den Schlüssel für mehrere Regionen AWS KMS

  Ihr AWS KMS Schlüssel erfordert eine wichtige Richtlinie. Stellen Sie sich eine ähnliche wichtige Richtlinie vor, die den Zugriff auf Prinzipale (Benutzer und Rollen) beschränkt, die über Berechtigungen verfügen, die mit dem Verwaltungskonto Ihrer Organisation verknüpft sind:

  JSON

```
{
    "Version":"2012-10-17",
    "Id": "KMS key policy",
    "Statement": [
        {
            "Sid": "Enable IAM User Permissions",
```

```
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:root"
            },
            "Action": "kms:*",
            "Resource": "*"
        },
        {
            "Sid": "Allow use of the KMS key for organization",
            "Effect": "Allow",
            "Principal": {
                "AWS": "*"
            },
            "Action": [
                "kms:Decrypt",
                "kms:DescribeKey",
                "kms:GenerateDataKey*",
                "kms:Encrypt",
                "kms:ReEncrypt*",
                "kms:GetKeyPolicy",
                "kms:CreateGrant",
                "kms:ListGrants",
                "kms:RevokeGrant"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:PrincipalOrgID": "ORGANIZATION-ID"
                }
            }
        }
    ]
}
```

Diese Beispielrichtlinie gewährt allen Konten in Ihrer Organisation Zugriff auf ihre verschlüsselten Backup-Daten. Verwenden Sie AWS globale Bedingungsschlüssel und AWS KMS Bedingungsschlüssel, um die Berechtigungen zu verfeinern, je nachdem, welche Prinzipale Zugriff auf Ihre Backups benötigen.

> **Note**
>
> Ihr AWS KMS Schlüssel für mehrere Regionen muss für jeden Schlüssel repliziert werden AWS-Region , den Sie mit AWS Control Tower verwalten möchten. Sie müssen für jeden Replikatschlüssel mit mehreren Regionen eine Schlüsselrichtlinie festlegen. Informationen zum Erstellen von Replikatschlüsseln finden Sie unter Replikatschlüssel für mehrere Regionen erstellen.

Backups aktivieren

Sie können Backups für Ressourcen in Ihren Konten aktivieren, die bei AWS Control Tower registriert sind, entweder während der Einrichtung der landing zone oder wenn Sie Ihre landing zone aktualisieren.

Als Voraussetzungen, Sie müssen die folgenden Artikel bereitstellen

- Und AWS-Konto um als AWS Backup Administratorkonto zu dienen
- Ein AWS-Konto , das als AWS Backup zentrales Backup-Konto dient
- Ein AWS KMS Schlüssel für mehrere Regionen, den Sie verwalten, für kontoübergreifende Backups

Wie aktiviert man Backups

Der Aktivierungsprozess besteht aus zwei Hauptteilen: Aktivieren Sie zunächst Backups für Ihre landing zone; aktivieren Sie dann Backups für jede registrierte Organisationseinheit, die Backups benötigt.

Erster Teil: Richten Sie Backups für Ihre landing zone ein

Konsole: Sie können Backups für Ihre landing zone in der AWS Control Tower Tower-Konsole auf der Seite mit den Landingzone-Einstellungen einrichten. Diese Option wird dir bei der ersten Einrichtung der landing zone angezeigt und du kannst sie später mit einem Update der landing zone erneut aufrufen.

API: Sie können Backups mit den AWS Control Tower-APIs aktivieren, indem Sie die `UpdateLandingZone`API aufrufen, wenn Sie bereits eine AWS Control Tower Tower-Landezone

haben, oder die `CreateLandingZone`API, wenn Sie AWS Control Tower zum ersten Mal einrichten. (Hinweis: Rufen Sie danach die `EnableBaseline`API auf, um Backups für jede benötigte Organisationseinheit zu erstellen.)

Außerhalb der AWS Control Tower Tower-Konsole

Ein Teil der Aktivierung von Backups für Ihre landing zone beinhaltet einen Schritt außerhalb der AWS Control Tower Tower-Konsole. Sie müssen zur AWS Backup Konsole navigieren, um Ihre Ressourcen zu überprüfen.

Um die Ressourcentypen zu überprüfen, für die Sie sich entschieden haben, oder um zusätzliche Ressourcentypen zu aktivieren

1. Öffnen Sie die Konsole unter. AWS Backup https://console.aws.amazon.com/backup
2. Wählen Sie im Navigationsbereich Settings (Einstellungen).
3. Wählen Sie auf der Seite Service opt-in (Service-Opt-In) die Option Configure resources (Ressourcen konfigurieren) aus.
4. Verwenden Sie die Kippschalter, um die Dienste zu aktivieren oder zu deaktivieren, die Sie AWS Backup einbinden möchten. Stellen Sie sicher, dass die Ressourcen, die Sie sichern möchten, ausgewählt sind, z. B. RDS, EC2, DDB usw., unabhängig davon, ob sie Teil Ihrer AWS Control Tower Tower-Umgebung sind oder nicht.

Weitere Informationen finden Sie unter Opt-In to Managing Services with. AWS Backup

> **Überlegungen zu neuen Ressourcentypen**
>
> Bevor Sie sich AWS Backup darauf verlassen, den Datenschutz für die Ressourcen eines AWS Dienstes zu verwalten, müssen Sie das vorherige Verfahren ausführen und sich AWS Backup für diesen Dienst entscheiden. Da der AWS Backup Service in future zusätzliche Services und deren Ressourcentypen unterstützt, müssen Sie dieses Verfahren wiederholen und sich für jeden weiteren Ressourcentyp mit anmelden, AWS Backup bevor Sie diesen Ressourcentyp in AWS Control Tower sichern können. Das Markieren eines nicht unterstützten Ressourcentyps kann dazu führen, dass Ihre Sicherung fehlschlägt.

Wenn Sie Backups für Ihre landing zone aktivieren, richtet AWS Control Tower die beiden Konten ein, die Sie als Central Backup-Konto bzw. als Backup-Administratorkonto angegeben haben. AWS Control Tower erstellt Ressourcen in diesen und anderen Konten.

> **Important**
>
> Um Backups für die AWS Control Tower Audit - und Log Archive-Konten zu aktivieren, müssen Sie Backups für die Security OU einrichten, indem Sie die `EnableBaseline` API aufrufen. Wir empfehlen Ihnen, dies zu tun.

Die empfohlenen Pläne und Aufbewahrungsmöglichkeiten lauten wie folgt:

- Stündliche Backups = 2-wöchige Aufbewahrung im lokalen Tresor, keine Kopie im zentralen Backup-Tresor
- Tägliche Backups = 2-wöchige Aufbewahrung im lokalen Tresor, 1-monatige Aufbewahrung im zentralen Backup-Tresor
- Wöchentliche Backups = 1 Monat Aufbewahrung im lokalen Tresor, 3 Monate Aufbewahrung im zentralen Tresor
- Monatliche Backups = 3-monatige Aufbewahrung im lokalen Tresor, 3-monatige Aufbewahrung im zentralen Backup-Tresor

Informationen zur Erstellung Ihrer Backup-Pläne finden Sie unter Berichtspläne mit der AWS Backup Konsole erstellen.

Nächster Teil: Backups auf Organisationseinheiten aktivieren

Nachdem Sie die Aktivierung AWS Backup in Ihren landing zone Zone-Einstellungen vorgenommen haben, müssen Sie den zusätzlichen Schritt ausführen, um das Backup für die spezifischen Organisationseinheiten zu aktivieren, die Sie sichern möchten. Wenn Sie die Option AWS Backup für Ihre landing zone aktiviert haben, wird auf der Seite mit den OU-Details in der Konsole ein Abschnitt angezeigt, in dem Sie Backup für die OU aktivieren auswählen können. Wenn das Backup auf Landingzone-Ebene nicht aktiviert ist, wird dieser Abschnitt auf der Seite mit den OU-Details nicht angezeigt.

Um das `BackupBaseline` auf einer Organisationseinheit zu aktivieren, muss es in dieser Organisationseinheit bereits `AWSControlTowerBaseline` aktiviert sein. Für registrierte Konten in jeder Organisationseinheit `AWSControlTowerBaseline` ist das aktiviert.

In Ihren ausgewählten Konten und Organisationseinheiten richtet AWS Control Tower zusätzliche Ressourcen ein

- Ein lokaler Backup-Tresor

  AWS Control Tower erstellt einen lokalen Backup-Tresor in Ihren Konten, wobei vier mögliche Arten von Backup-Plänen an den Tresor angehängt sind. Über AWS Control Tower erstellte Backup-Pläne sind mit einem Präfix gekennzeichnet.

```
BackupPlanTags:
        aws-control-tower: 'managed-by-control-tower'
```

- Vier Arten von Backup-Plänen — stündlich, täglich, wöchentlich, monatlich.

  Jeder Plan ist mit einer tagbasierten Ressourcenzuweisung verknüpft. Beispielsweise ist jede Ressource, die mit aws-control-tower-backuphourly: true gekennzeichnet ist, durch einen stündlichen Sicherungsplan geschützt.

- Eine lokale Backup-Rolle in Ihren Konten

  AWS Control Tower erstellt eine IAM-Rolle, die für Backups verwendet wird. Für die Rolle sind vier spezifische Berechtigungen erforderlich.

```
"backup:UpdateGlobalSettings","organizations:RegisterDelegatedAdministrator","organizations:E
```

  Die Rolle hat eine Vertrauensbeziehung mit dem Dienstprinzipal für AWS Backup Die Rolle trägt den Name`aws-controltower-backup-role`, und ihr sind die folgenden verwalteten Berechtigungen zugeordnet:

  - `AWSBackupServiceRolePolicyForBackup`
  - `AWSBackupServiceRolePolicyForRestores`
  - `AWSBackupServiceRolePolicyForS3Backup`
  - `AWSBackupServiceRolePolicyForS3Restore`

Ressourcen für Backups kennzeichnen

Ein Teil der Einrichtung von Backups in AWS Control Tower besteht darin, die Ressourcen zu kennzeichnen, die Sie in Ihren Backup-Plan aufnehmen möchten. Die Tags geben die Häufigkeit der Backups an. Dies sind die möglichen Tags.

- `aws-control-tower-backuphourly : true`
- `aws-control-tower-backupdaily: true`
- `aws-control-tower-backupweekly: true`
- `aws-control-tower-backupmonthly: true`

Überlegungen

- Wenn auf einer OU aktiv AWS Backup ist, wird im Feld Status auf der Seite mit den OU-Details in der AWS Control Tower Tower-Konsole der Wert Aktiviert angezeigt. Zu den anderen möglichen Werten des Felds Status gehören Nicht aktiviert, In Bearbeitung und Fehlgeschlagen. Wenn der Status Fehlgeschlagen angezeigt wird, wählen Sie Re-register OU aus, um Ihre AWS Backup Konfiguration erneut auf die OU anzuwenden.
- Wenn Sie die AWS Backup Aktivierung auf einer Organisationseinheit aktiviert haben, werden neue Konten, die über Account Factory bereitgestellt wurden, unter dieser Organisationseinheit enthalten AWS Backup.

Schalten Sie Backups aus

Sie können Backups für Ihre Ressourcen in Konten deaktivieren, die bei AWS Control Tower registriert sind, entweder während der Einrichtung der landing zone oder wenn Sie Ihre landing zone aktualisieren.

Zum Deaktivieren von Backups sind zwei Hauptschritte erforderlich: Schalten Sie zunächst die AWS Backup Baseline auf jeder Organisationseinheit aus, für die Backups aktiviert sind, und deaktivieren Sie dann die Backups für Ihre landing zone.

Erster Schritt: Schalten Sie Backups auf Organisationseinheiten aus

Wenn AWS Backup aktiviert, müssen Sie die AWS Backup Baseline für alle Organisationseinheiten deaktivieren, bevor Sie sie AWS Backup für Ihre landing zone ausschalten können.

Wenn Sie verschachtelte Organisationseinheiten haben, deaktivieren Sie die AWS Backup Backup-Baseline für die untergeordneten Organisationseinheiten vor der übergeordneten Organisationseinheit. Während die AWS Backup Backup-Baseline auf einer untergeordneten Organisationseinheit immer noch aktiviert ist, kann AWS Control Tower sie auf der übergeordneten Organisationseinheit nicht deaktivieren.

Sie können die AWS Backup Backup-Baseline auf einer Organisationseinheit mithilfe der AWS Control Tower Tower-APIs oder der AWS Control Tower Tower-Konsole deaktivieren.

So deaktivieren Sie die AWS Backup Backup-Baseline (API)

Suchen Sie zunächst den ARN der AWS Backup Backup-Baseline. Rufen Sie die `ListBaselines` API auf und fragen Sie nach der Baseline ab, deren ARN abgerufen werden `name` `BackupBaseline` soll.

```
aws controltower list-baselines --query 'baselines[?name==`BackupBaseline`]'
```

Identifizieren Sie dann anhand dieses ARN, für welche Organisationseinheiten die AWS Backup Backup-Baseline aktiviert ist. Rufen Sie die `ListEnabledBaselines` API auf und filtern Sie nach der `BackupBaseline` Baseline-ID, um jede aktivierte Baseline und ihren `enabledBaselineIdentifier` ARN zu deaktivieren.

```
aws controltower list-enabled-baselines --filter baselineIdentifiers=BackupBaseline-ARN
```

Um die AWS Backup Backup-Baseline auf einer Organisationseinheit zu deaktivieren, können Sie die `DisableBaseline` API aufrufen.

Beispielbefehl:

```
aws controltower disable-baseline --enabled-baseline-identifier Enabled-baseline-ARN
```

So deaktivieren Sie die AWS Backup Backup-Baseline (Konsole)

1. Melden Sie sich bei der AWS Control Tower Tower-Konsole an und navigieren Sie zur Organisationsseite.
2. Wählen Sie die Organisationseinheit aus, deren AWS Backup Backup-Basisstatus Aktiviert ist, um die OU-Detailseite zu öffnen.
3. Wählen Sie im Abschnitt Integrationen in dieser OU — optional unter AWS Backup die Option Bearbeiten aus.
4. Wählen Sie im daraufhin angezeigten Dialogfeld Deaktivieren und anschließend Bestätigen aus.

Wenn Sie die AWS Backup Baseline deaktivieren, bereinigt AWS Control Tower die folgenden Ressourcen:

- Alle Stacksets beziehen sich auf AWS Backup
- Alle Steuerelemente beziehen sich auf AWS Backup

> **Note**
>
> Der lokale Tresor wird beibehalten, obwohl die Stacksets gelöscht wurden, da die Aufbewahrungsrichtlinie für den lokalen Tresor auf eingestellt ist. `Retain` Es bewahrt Ihre Daten.

Nächster Schritt: Ausschalten AWS Backup für deine landing zone

Wenn die Voraussetzung erfüllt ist, indem Sie Backups für Ihre Organisationseinheiten deaktiviert haben, navigieren Sie zur Einstellungsseite der Landing Zone, um Backups von der AWS Control Tower Tower-Konsole aus zu deaktivieren. Wählen Sie Backup deaktivieren.

Wenn Sie das Gerät ausschalten AWS Backup, ändert AWS Control Tower die folgenden Ressourcen:

- Entfernt alle Stacksets im Zusammenhang mit AWS Backup
- Deaktiviert alle Steuerelemente, die sich auf die AWS Backup Sicherheits-OU beziehen
- De-registers das delegierte Administratorkonto für die Verwaltung AWS Backup
- Entfernt die AWS Control Tower Tower-Governance (für CloudTrail AWS Config, usw.) aus den AWS Backup Administrator- und Central Backup-Konten
- AWS Control Tower behält die AWS Backup Tresore und Amazon S3 S3-Bucket-Ressourcen, die Ihre Daten enthalten

Nachdem Sie Backups deaktiviert haben, werden keine neuen Backups erstellt, aber bestehende Backups werden nicht entfernt.

Aktivieren Sie die Sicherung für verschobene Konten

Wenn Sie ein Konto in eine AWS Backup aktivierte AWS Control Tower-Organisationseinheit verschieben und das Konto nicht bei AWS Control Tower registriert ist, gilt Ihr Backup-Plan nicht automatisch für das Konto.

Konsole: Um die Aktivierung AWS Backup für ein einzelnes Konto von der AWS Control Tower Tower-Konsole aus zu aktivieren, können Sie auf der Seite mit den Kontodetails die Option Konto aktualisieren auswählenRe-register , oder Sie können auf der Seite mit den OU-Details die Option OU auswählen, um mehrere Konten gleichzeitig zu aktualisieren.

API: Wenn Sie über die API ein Konto in eine Organisationseinheit verschieben, für die die Backup-Baseline aktiviert ist, können Sie die `ResetEnabledBaseline` API in dieser OU aufrufen und dabei die `EnabledBaseline` Ressource der Organisationseinheit als Ziel angeben, um Backups auf dem Konto durch Vererbung von der OU auszulösen.

Beispielbefehl:

```
aws controltower reset-enabled-baseline --enabled-baseline-identifier
 arn:aws:controltower:REGION:NAMESPACE:enabledbaseline/XOSDORW8HDB5ZNWEE --region us-
east-1
```

Beispielantwort:

```
{
        "operationIdentifier": "0bbdb587-c849-4152-95c6-7afa7664ee71"
}
```

Backup-Drift im AWS Control Tower

Drift wird für AWS Backup Konfigurationen in AWS Control Tower nicht gemeldet. Weitere Informationen zu Abweichungen in AWS Control Tower finden Sie unter Drift in AWS Control Tower erkennen und beheben.

Wenn Sie den AWS Backup Plan löschen oder ändern, kann Ihr Plan in den Status Drift übergehen. Hier sind einige Änderungen, die Sie vermeiden sollten.

- Verschieben Sie das Backup-Administratorkonto nicht aus der Security OU.
- Verschieben Sie das Central Backup-Konto nicht aus der Security OU.
- Entfernen Sie das Backup-Administratorkonto nicht aus der Organisation.
- Entfernen Sie das Central Backup-Konto nicht aus der Organisation.
- Trennen Sie das auf die Sicherheits-OU angewendete AWS Backup SCP nicht, fügen Sie es nicht an oder aktualisieren Sie es nicht.

- Das auf andere Organisationseinheiten angewendete AWS Backup SCP darf nicht getrennt, angehängt oder aktualisiert werden.
- Entfernen Sie nicht die Erlaubnis des Backup-Administratorkontos für AWS Backup.
- Aktualisieren Sie Ihre kontoübergreifenden Backup-Einstellungen nicht, um kontoübergreifende Backups zu deaktivieren. Weitere Informationen zu kontoübergreifenden Backups finden Sie *UpdateGlobalSettings*in der AWS Backup API-Referenz.
- Löschen Sie Ihren AWS KMS Schlüssel nicht.
- Ändern Sie Ihre AWS KMS Schlüsselrichtlinie nicht, nachdem sie festgelegt wurde.
- Deaktivieren Sie nicht den vertrauenswürdigen Zugriff des Dienstes für AWS Backup.

> **Note**
>
> Es wird ein Drift in Bezug auf den Status der SCP-based Kontrollen zum Schutz der AWS Backup Ressourcen in AWS Control Tower gemeldet.

Ressourcen erstellt für AWS Backup

Die Tabellen auf dieser Seite zeigen Ressourcen, die bei der Aktivierung in AWS Control Tower Tower-Konten erstellt AWS Backup werden.

Die folgende Tabelle zeigt die Ressourcen, die AWS Control Tower im AWS Control Tower Central Backup-Konto erstellt, wenn Sie es AWS Backup für die landing zone Zone-Organisation aktivieren.

Beschreibung	Ressourcen für das Central Backup-Konto
Welche Organisationseinheit enthält das Konto?	Sicherheits-OU
Durch welche Aktion wurde die Ressource erstellt?	Landezone: Erstellen oder aktualisieren
Welche Ressourcen werden erstellt?	Zentraler Backup-Tresor— `aws-controltower-central-backupvault-*`
Welche Regionen sind enthalten?	Alle regierten Regionen

Beschreibung	Ressourcen für das Central Backup-Konto
Welche Kontrollen stehen im Zusammenhang mit diesen Ressourcen?	`CT.BACKUP.PV.3`

Die folgende Tabelle zeigt die Ressourcen, die AWS Control Tower im AWS Control Tower Backup-Administratorkonto erstellt, wenn Sie es AWS Backup für die landing zone Zone-Organisation aktivieren.

Beschreibung	Ressourcen für das Backup-Administratorkonto: Dies ist das delegierte Administratorkonto für AWS Backup
Welche Organisationseinheit enthält das Konto?	Sicherheits-OU
Durch welche Aktion wurde die Ressource erstellt?	Landezone: Erstellen oder aktualisieren
Welche Ressourcen werden erstellt?	Backup-Auditmanager (BAM) • `aws_controltower_copy_report` • `aws_controltower_backup_report` • `aws_controltower_restore_report` Amazon S3 S3-Bucket zum Speichern von BAM-Protokollen— `aws-controltower-backup-reports-` *`{accountId}`* `-*` Amazon S3 S3-Bucket für die Zugriffsprotokollierung— `aws-controltower-backup-reports-log-` *`{accountId}`* `-*`
Welche Regionen sind enthalten?	Heimatregion

Beschreibung	Ressourcen für das Backup-Administrat orkonto: Dies ist das delegierte Administr atorkonto für AWS Backup
Welche Kontrollen stehen im Zusammenhang mit diesen Ressourcen?	• `CT.BACKUP.PV.2` • `CT.S3.PV.1` • `CT.S3.PV.1`

Die folgende Tabelle zeigt die Ressourcen, die AWS Control Tower im AWS Control Tower Audit-Konto und im AWS Control Tower Log Archive-Konto erstellt, wenn Sie sie AWS Backup für die Security OU aktivieren.

Beschreibung	Ressourcen für Audit- und Log Archive-Konten
Welche Organisationseinheit enthält das Konto?	Sicherheits-OU
Durch welche Aktion wurde die Ressource erstellt?	Aktivierung der `BackupBaseline`

Welche Ressourcen werden geschaffen?	• Lokaler Backup-Tresor— `aws-controltower-local-backupvault-*`
	• Rolle „Lokales Backup “— `aws-controltower-BackupRole`
	• Vier lokale Backup-Pläne (stündlich, wöchentlich, monatlich, täglich)
	  • `aws-controltower-hourly-backup-plan`
	  • `aws-controltower-daily-backup-plan`
	  • `aws-controltower-weekly-backup-plan`
	  • `aws-controltower-monthly-backup-plan`

Beschreibung	Ressourcen für Audit- und Log Archive-Konten
	• Eine IAM-Rolle— `aws-controltower-BackupRole`
Welche Regionen sind enthalten?	Alle regierten Regionen
Welche Kontrollen stehen im Zusammenhang mit diesen Ressourcen?	• `CT.BACKUP.PV.3` • `CT.IAM.PV.1` • `CT.BACKUP.PV.3` • `CT.BACKUP.PV.1`

> **Note**
>
> Wenn Sie das `BackupBaseline` auf die Sicherheitsorganisationseinheit anwenden, erhalten alle Mitgliedskonten in dieser Organisationseinheit die AWS Backup Ressourcen, nicht nur die Konten Audit und Log Archive.

Die folgende Tabelle zeigt die Ressourcen, die AWS Control Tower in den Mitgliedskonten der AWS Control Tower OU erstellt, wenn Sie sie AWS Backup auf einer Ziel-OU aktivieren.

Beschreibung	Ressourcen für Mitgliedskonten in anderen OUs
Welche Organisationseinheit enthält das Konto?	Jede Organisationseinheit außer der Sicherheits-Organisationseinheit
Durch welche Aktion wurde die Ressource erstellt?	Aktivierung der `BackupBaseline`
Welche Ressourcen werden geschaffen?	• Lokaler Backup-Tresor— `aws-controltower-local-backupvault-*` • Rolle „Lokales Backup “— `aws-controltower-BackupRole` • Vier lokale Backup-Pläne (stündlich, wöchentlich, monatlich, täglich)

Beschreibung	Ressourcen für Mitgliedskonten in anderen OUs
	• `aws-controltower-hourly-backup-plan` • `aws-controltower-daily-backup-plan` • `aws-controltower-weekly-backup-plan` • `aws-controltower-monthly-backup-plan` • Eine IAM-Rolle— `aws-controltower-BackupRole`
Welche Regionen sind enthalten?	Alle regierten Regionen
Welche Kontrollen stehen im Zusammenhang mit diesen Ressourcen?	• `CT.BACKUP.PV.3` • `CT.IAM.PV.1` • `CT.BACKUP.PV.3` • `CT.BACKUP.PV.1`

Kontrollen für AWS Backup

Wenn Sie AWS Backup in Ihrer AWS Control Tower Tower-Landezone aktivieren, werden einige präventive Kontrollen in Ihrer Umgebung aktiviert. Diese Kontrollen schützen die Ressourcen, die AWS Backup für den Betrieb mit AWS Control Tower erforderlich sind. Sie können diese Steuerelemente nicht aktivieren, wenn AWS Backup sie für Ihre landing zone nicht aktiviert sind.

Weitere Informationen finden Sie unter Steuerungen für AWS Backup.

Außerbetriebnahme einer AWS Control Tower Tower-Landezone

Mit AWS Control Tower können Sie sichere AWS Umgebungen mit mehreren Konten einrichten und verwalten, die als Landing Zones bezeichnet werden. Der Vorgang der Bereinigung aller vom AWS Control Tower zugewiesenen Ressourcen wird als Außerbetriebnahme einer landing zone bezeichnet.

Wenn Sie AWS Control Tower nicht mehr verwenden möchten, bereinigt das automatisierte Tool zur Außerbetriebnahme die von AWS Control Tower zugewiesenen Ressourcen. Um den automatisierten Außerbetriebnahmeprozess zu starten, navigieren Sie zur Seite landing zone Settings, wählen Sie die Registerkarte Außerbetriebnahme und anschließend Landingzone außer Betrieb nehmen.

Eine Liste der während der Außerbetriebnahme durchgeführten Aktionen finden Sie unter. Überblick über den Außerbetriebnahmeprozess

> **Warning**
>
> Das manuelle Löschen all Ihrer AWS Control Tower Tower-Ressourcen ist nicht dasselbe wie eine Außerbetriebnahme. Sie können damit keine neue landing zone einrichten.

Ihre Daten und Ihre vorhandenen Daten AWS Organizations werden durch den Stilllegungsprozess auf folgende Weise nicht geändert.

- AWS Control Tower entfernt nicht Ihre Daten, sondern nur Teile der Landing Zone, die AWS Control Tower erstellte.
- Nach Abschluss des Außerbetriebnahmevorgangs verbleiben einige Ressourcenartefakte wie Amazon S3 S3-Buckets und Amazon CloudWatch Logs-Protokollgruppen. Diese Ressourcen müssen manuell gelöscht werden, bevor Sie eine weitere Landing Zone einrichten, um mögliche Kosten im Zusammenhang mit dem Beibehalten bestimmter Ressourcen zu vermeiden.
- Sie können die automatische Außerbetriebnahme nicht verwenden, um eine teilweise eingerichtete Landing Zone zu entfernen. Wenn der Einrichtungsprozess für die Landing Zone fehlschlägt, müssen Sie den Fehlerstatus beheben und die Landing Zone vollständig neu einrichten, um eine automatische Außerbetriebnahme zu ermöglichen. Andernfalls müssen Sie die Ressourcen einzeln löschen.

Das Außerbetriebnehmen einer Landing Zone ist ein Prozess mit erheblichen Auswirkungen und kann nicht rückgängig gemacht werden. Die von AWS Control Tower ergriffenen Maßnahmen zur Außerbetriebnahme und die Artefakte, die nach der Außerbetriebnahme verbleiben, werden in den folgenden Abschnitten beschrieben.

> **Important**
>
> Wir empfehlen Ihnen dringend, diesen Außerbetriebnahmeprozess nur dann durchzuführen, wenn Sie beabsichtigen, Ihre Landing Zone nicht mehr zu verwenden. Es ist nicht möglich, Ihre bestehende Landing Zone neu zu erstellen, nachdem Sie sie außer Betrieb genommen haben.

Überblick über den Außerbetriebnahmeprozess

Wenn Sie die Außerbetriebnahme Ihrer landing zone beantragen, führt AWS Control Tower die folgenden Aktionen aus.

- Deaktiviert jede Detective Control, die in der landing zone aktiviert ist. AWS Control Tower löscht die CloudFormation Ressourcen, die die Steuerung unterstützen.
- Deaktiviert jede präventive Kontrolle, indem Service Control Policies (SCPs) von entfernt werden. AWS Organizations Wenn eine Richtlinie leer ist (was nach dem Entfernen aller von AWS Control Tower verwalteten SCPs der Fall sein sollte), trennt AWS Control Tower die Richtlinie und löscht sie vollständig.
- Löscht alle Blueprints, die bereitgestellt werden als. CloudFormation StackSets
- Löscht alle Blueprints, die als CloudFormation Stacks in allen Regionen bereitgestellt wurden.
- Für jedes bereitgestellte Konto führt AWS Control Tower während der Außerbetriebnahme die folgenden Aktionen durch.
  - Es werden die Datensätze jedes Account Factory-Kontos gelöscht.
  - Widerruft die AWS Control Tower-Berechtigungen für das Konto, indem die von AWS Control Tower erstellte IAM-Rolle entfernt wird (sofern ihr keine zusätzlichen Richtlinien hinzugefügt wurden) und die `OrganizationAccountAccessRole` Standard-IAM-Rolle neu erstellt.
  - Entfernt Aufzeichnungen des Kontos von. AWS Service Catalog
  - Es wird das Account Factory-Produkt und Portfolio von AWS Service Catalog entfernt.
- Löscht die Blueprints für die gemeinsamen Konten (Audit und Log Archive).

- Widerruft die AWS Control Tower-Berechtigungen für die gemeinsam genutzten Konten, indem die von AWS Control Tower erstellte IAM-Rolle entfernt wird (sofern ihr keine zusätzlichen Richtlinien hinzugefügt wurden) und die `OrganizationAccountAccessRole` IAM-Rolle neu erstellt.
- Löscht Datensätze, die sich auf die gemeinsamen Konten beziehen.
- Es werden die Datensätze gelöscht, die sich auf die vom Kunden erstellten OUs beziehen.
- Es werden die internen Datensätze gelöscht, mit denen die „Home“-Region identifiziert wird.

> **Note**
>
> Nach der Außerbetriebnahme können Sie die Account Factory VPC-Vorlage (`BP_ACCOUNT_FACTORY_VPC`) entfernen, um die Routen und NAT-Gateways zu bereinigen, wenn Ihre VPC nicht leer war.

Wie man eine landing zone außer Betrieb nimmt

Gehen Sie wie hier beschrieben vor, um Ihre AWS Control Tower Tower-Landezone von der Konsole aus außer Betrieb zu nehmen.

> **Note**
>
> Wir empfehlen Ihnen, die Verwaltung Ihrer registrierten Konten vor der Außerbetriebnahme aufzuheben.

1. Wenn die AWS Backup Backup-Baseline auf einer registrierten OU aktiviert ist, deaktivieren Sie sie auf jeder OU, in der sie aktiviert ist, bevor Sie Ihre Landing Zone außer Betrieb nehmen. Andernfalls schlägt die Außerbetriebnahme fehl. Detaillierte Anweisungen finden Sie unter the section called “Erster Schritt: Schalten Sie Backups auf Organisationseinheiten aus”.

   Wenn die Außerbetriebnahme aus diesem Grund bereits fehlgeschlagen ist, können Sie die AWS Backup Backup-Baseline deaktivieren und die Außerbetriebnahme erneut ausführen.
2. Navigieren Sie in der AWS Control Tower Tower-Konsole zur Seite Landing Zone Settings.
3. Wählen Sie im Abschnitt landing zone stilllegen die Option landing zone außer Betrieb setzen.

4. Es erscheint ein Dialog mit einem erforderlichen Bestätigungsvorgang, in dem die Aktion, die Sie durchführen wollen, erklärt wird. Um zu bestätigen, dass die gewünschte Außerbetriebnahme erfolgen soll, müssen Sie jedes Feld markieren und die Bestätigung wie gewünscht eingeben.

   > **Important**
   >
   > Der Außerbetriebnahmeprozess kann nicht rückgängig gemacht werden.

5. Wenn Sie Ihre Absicht bestätigen, Ihre landing zone Betrieb zu nehmen, werden Sie während der Außerbetriebnahme auf die AWS Control Tower Tower-Startseite weitergeleitet. Der Prozess kann bis zu zwei Stunden dauern.

   Schließen Sie während der Außerbetriebnahme keine Mitgliedskonten in Ihrer Organisation. Die Außerbetriebnahme schlägt möglicherweise fehl.

6. Wenn die Außerbetriebnahme erfolgreich war, müssen Sie die verbleibenden Ressourcen manuell löschen, bevor Sie über die AWS Control Tower Tower-Konsole eine neue landing zone einrichten. Zu diesen verbleibenden Ressourcen gehören einige spezifische Amazon S3 S3-Buckets, Organisationen und CloudWatch Logs-Protokollgruppen.

   > **Note**
   >
   > Diese Maßnahmen können erhebliche Auswirkungen auf Ihre Abrechnungs- und Compliance-Aktivitäten haben. Wenn diese Ressourcen beispielsweise nicht gelöscht werden, kann dies zu unerwarteten Gebühren führen.

   Weitere Informationen zum manuellen Löschen von Ressourcen finden Sie unter Über das Entfernen von AWS Control Tower Tower-Ressourcen.

7. Wenn Sie beabsichtigen, eine neue landing zone in einer neuen AWS Region einzurichten, folgen Sie diesem zusätzlichen Schritt. Geben Sie den folgenden Befehl über die CLI ein:

```
aws organizations disable-aws-service-access --service-principal
 controltower.amazonaws.com
```

Machen Sie Ihre landing zone mit APIs außer Betrieb

Der Vorgang der Säuberung aller Ressourcen einer landing zone wird als Stilllegung einer Landezone bezeichnet.

> **Important**
>
> Wir empfehlen Ihnen dringend, diesen Außerbetriebnahmeprozess nur dann durchzuführen, wenn Sie beabsichtigen, Ihre Landing Zone nicht mehr zu verwenden. Es ist nicht möglich, Ihre bestehende Landing Zone neu zu erstellen, nachdem Sie sie außer Betrieb genommen haben.

Weitere Informationen zur Außerbetriebnahme einer landing zone, einschließlich wichtiger Informationen darüber, wie AWS Control Tower mit Ihren und bestehenden Daten umgeht AWS Organizations, finden Sie unter. Außerbetriebnahme einer AWS Control Tower Tower-Landezone

Rufen Sie `DeleteLandingZone` API auf, um eine landing zone außer Betrieb zu nehmen. Diese API gibt eine zurück`OperationIdentifier`, die Sie dann verwenden können, wenn Sie die `GetLandingZoneOperation` API aufrufen, um den Status des Löschvorgangs zu überprüfen.

```
aws controltower delete-landing-zone --landing-zone-identifier
"arn:aws:controltower:us-west-2:123456789012:landingzone/1A2B3C4D5E6F7G8H"
```

Ausgabe:

```
{
   "operationIdentifier": "55XXXXXX-e2XX-41XX-a7XX-446XXXXXXXXX"
}
```

Nach der Außerbetriebnahme sind manuelle Aufräumarbeiten erforderlich

In diesem Abschnitt werden manuelle Bereinigungsaufgaben aufgeführt, die Sie nach dem ersten Schritt der Außerbetriebnahme ausführen müssen.

- Sie müssen unterschiedliche E-Mail-Adressen für die Konten Log Archive und Audit angeben, wenn Sie nach der Außerbetriebnahme eine neue landing zone einrichten, oder Sie müssen das Verfahren befolgen, um Ihre eigenen bestehenden Log-Archiv- oder Audit-Konten mitzunehmen.
- Die Protokollgruppe CloudWatch Logs,`aws-controltower/CloudTrailLogs`, muss manuell gelöscht werden, bevor Sie eine weitere landing zone einrichten.
- Die beiden Amazon S3 S3-Buckets mit reservierten Namen für Protokolle müssen manuell entfernt oder umbenannt werden.
- Sie müssen die vorhandenen Security - und Sandbox-Organisationseinheiten manuell löschen oder umbenennen.

> **Note**
>
> Bevor Sie die Organisation der AWS Control Tower Security OU löschen können, müssen Sie zunächst die Protokollierungs- und Auditkonten löschen, nicht jedoch das Verwaltungskonto. Um diese Konten zu löschen, müssen Sie die Wann sollten Sie sich als Root-Benutzer anmelden beim Prüfungskonto und Protokollierungskonto vornehmen und diese einzeln löschen.

- Möglicherweise möchten Sie die AWS IAM Identity Center (IAM Identity Center) -Konfiguration für AWS Control Tower manuell löschen, aber Sie können mit der vorhandenen IAM Identity Center-Konfiguration fortfahren.
- Möglicherweise möchten Sie die von AWS Control Tower erstellte VPC und das zugehörige AWS CloudFormation Stack-Set entfernen.
- Bevor Sie eine neue landing zone in einer neuen AWS Region einrichten können, müssen Sie die folgenden zusätzlichen Schritte ausführen.
  - Geben Sie den folgenden Befehl über die CLI ein:

```
aws organizations disable-aws-service-access --service-principal
 controltower.amazonaws.com
```

  - Löschen Sie die verbleibende verwaltete Regel (genannt`AWSControlTowerManagedRule`) aus den gemeinsamen Konten und Mitgliedskonten für alle verwalteten Regionen. `AWSControlTowerManagedRule`ist eine EventBridge Amazon-Regel.

Ressourcen, die bei der Außerbetriebnahme nicht entfernt wurden

Durch die Außerbetriebnahme einer landing zone wird der Einrichtungsprozess von AWS Control Tower nicht vollständig rückgängig gemacht. Bestimmte Ressourcen bleiben erhalten, die manuell entfernt werden können.

AWS Organizations

Für Kunden ohne bestehende AWS Organizations Organisationen richtet AWS Control Tower eine Organisation mit einer oder mehreren Organisationseinheiten (OUs) ein. Die angegebene Sicherheits-OU und optional die erstellte Sandbox-OU. Beim Bereitstellen Ihrer Landing Zone wird die Hierarchie der Organisation wie folgt beibehalten:

- Organisationseinheiten (OUs), die Sie über die AWS Control Tower Tower-Konsole erstellt haben, werden nicht entfernt.
- Die Sicherheits- und Sandbox-Organisationseinheiten werden nicht entfernt.
- Die Organisation wurde nicht aus AWS Organizations gelöscht.
- Es werden keine Konten in AWS Organizations (gemeinsam genutzt, bereitgestellt oder verwaltet) verschoben oder entfernt.

AWS IAM Identity Center (SSO)

Für Kunden ohne vorhandenes IAM Identity Center-Verzeichnis richtet AWS Control Tower das IAM Identity Center ein und konfiguriert ein erstes Verzeichnis. Wenn Sie Ihre landing zone außer Betrieb nehmen, nimmt AWS Control Tower keine Änderungen am IAM Identity Center vor. Bei Bedarf können Sie die in Ihrem Verwaltungskonto gespeicherten IAM Identity Center-Informationen manuell löschen. Durch die Außerbetriebnahme bleiben insbesondere diese Bereiche unverändert:

- Benutzer, die mit Account Factory angelegt wurden, werden nicht entfernt.
- Gruppen, die durch das AWS Control Tower Tower-Setup erstellt wurden, werden nicht entfernt.
- Von AWS Control Tower erstellte Berechtigungssätze werden nicht entfernt.
- Verknüpfungen zwischen AWS Konten und IAM Identity Center-Berechtigungssätzen werden nicht entfernt.
- Die IAM Identity Center-Verzeichnisse werden nicht geändert.
- Diese IAM Identity Center-Richtlinien für AWS Control Tower werden nicht entfernt:
  - `AWSControlTowerAdminPolicy`

- `AWSControlTowerCloudTrailRolePolicy`
- `AWSControlTowerStackSetRolePolicy`

Rollen

Während der Einrichtung erstellt AWS Control Tower bestimmte Rollen für Sie, wenn Sie die Konsole verwenden, oder er fordert Sie auf, diese Rollen zu erstellen, wenn Sie Ihre landing zone über die APIs einrichten. Wenn Sie Ihre landing zone außer Betrieb nehmen, werden die folgenden Rollen nicht entfernt:

- `AWSControlTowerAdmin`
- `AWSControlTowerCloudTrailRole`
- `AWSControlTowerStackSetRole`
- `AWSControlTowerConfigAggregatorRoleForOrganizations`

> **Note**
>
> Die `AWSControlTowerExecution` Rolle in den Mitgliedskonten wird gelöscht, wenn die landing zone gelöscht wird, unabhängig davon, ob AWS Control Tower die Rolle in Ihrem Namen erstellt hat oder ob Sie die Rolle manuell erstellt haben. Wenn Sie dieser Rolle jedoch zusätzliche Richtlinien angehängt oder die mit dieser Rolle verknüpften Richtlinien geändert haben, kann AWS Control Tower diese Rolle während des Löschens der Landing Zone möglicherweise nicht löschen. In solchen Fällen ist das Löschen der Landing Zone erfolgreich, aber die Rolle bleibt in Ihrem Mitgliedskonto erhalten.

Amazon-S3-Buckets

Während der Einrichtung erstellt AWS Control Tower Buckets im Protokollarchivkonto für AWS CloudTrail und im Config Central Aggregator-Konto für die AWS Config-Integration. AWS Control Tower erstellt Buckets für die Protokollierung und für die Protokollierung des Zugriffs in jedem dieser Konten. Bei der Außerbetriebnahme Ihrer Landing Zone werden die folgenden Ressourcen nicht entfernt:

- S3-Buckets für die Protokollierung und Protokollierung des Zugriffs im Protokollarchivkonto werden nicht entfernt.

- Die S3-Buckets für die Protokollierung und Protokollierung des Zugriffs im Config Central Aggregator-Konto werden nicht entfernt.
- Der Inhalt der Zugriffs-Buckets für Protokollierung und Protokollierung in jedem dieser Konten wird nicht entfernt.

Konten zur Serviceintegration

Für AWS Control Tower muss jede Service-Integrationskonfiguration über ein zentrales Konto verfügen. Dieses Konto kann während der Einrichtung von AWS Control Tower basierend auf der landing zone Zone-Version erstellt werden oder auch nicht. Dies geschieht, wenn Sie Ihre Landing Zone außer Betrieb nehmen:

- Serviceintegrationskonten, die während der Einrichtung von AWS Control Tower erstellt wurden, werden nicht geschlossen.
- Die `OrganizationAccountAccessRole` IAM-Rolle wird neu erstellt, um sie an die AWS Organizations Standardkonfiguration anzupassen.
- Die `AWSControlTowerExecution`-Rolle wird entfernt.

Bereitgestellte Konten

AWS Control Tower Tower-Kunden können Account Factory verwenden, um neue AWS Konten zu erstellen. Dies geschieht, wenn Sie Ihre Landing Zone außer Betrieb nehmen:

- Bereitgestellte Konten, die Sie mit Account Factory erstellt haben, werden nicht geschlossen.
- Bereitgestellte Produkte AWS Service Catalog werden nicht entfernt. Wenn Sie diese löschen, indem Sie sie kündigen, werden ihre Konten in die Root-Organisationseinheit verschoben.
- Die von AWS Control Tower erstellte VPC wird nicht entfernt, und das zugehörige AWS CloudFormation Stack-Set (`BP_ACCOUNT_FACTORY_VPC`) wird nicht entfernt.
- Die `OrganizationAccountAccessRole` IAM-Rolle wird neu erstellt, um sie an die Standardkonfiguration anzupassen. AWS Organizations
- Die `AWSControlTowerExecution`-Rolle wird entfernt.

CloudWatch Logs Protokollgruppe

- Eine CloudWatch Logs-Protokollgruppe`aws-controltower/CloudTrailLogs`,, wird als Teil des genannten `AWSControlTowerBP-BASELINE-CLOUDTRAIL-MASTER` Blueprints

erstellt. Diese Protokollgruppe wird nicht entfernt. Stattdessen wird die Vorlage gelöscht und die Ressourcen bleiben erhalten.

> **Note**
>
> Kunden mit landing zone 3.0 und höher müssen die CloudTrail Logs und CloudTrail Log-Rollen ihres individuellen registrierten Accounts nicht löschen, da diese nur im Verwaltungskonto für den Trail auf Organisationsebene erstellt werden.
> Ab landing zone Version 3.2 erstellt AWS Control Tower eine EventBridge Amazon-Regel namens`AWSControlTowerManagedRule`. Diese Regel wird in jedem Mitgliedskonto für alle regulierten Regionen erstellt. Die Regel wird bei der Außerbetriebnahme nicht automatisch gelöscht. Sie müssen sie daher manuell aus den Serviceintegrationskonten und Mitgliedskonten aller verwalteten Regionen löschen, bevor Sie eine landing zone in einer neuen Region einrichten können.

Verfahren zum Löschen von AWS Control Tower Tower-Ressourcen finden Sie unterAWS Control Tower Tower-Ressourcen entfernen.

AWS Control Tower Tower-Ressourcen entfernen

Dieses Dokument enthält Anweisungen zum individuellen Entfernen von AWS Control Tower Tower-Ressourcen im Rahmen regulärer Wartungs- und Verwaltungsaufgaben. Die in diesem Kapitel beschriebenen Verfahren dienen nur dazu, einzelne Ressourcen oder einige Ressourcen bei Bedarf zu entfernen. Es ist nicht dasselbe wie die Außerbetriebnahme Ihrer landing zone.

Bei zwei Arten von Aufgaben müssen Sie möglicherweise Ressourcen entfernen:

- Um Ressourcen zu löschen, während Sie Ihre Landing Zone in gewöhnlichen Situationen verwalten.
- Um Ressourcen zu bereinigen, die nach der automatisierten Außerbetriebnahme noch vorhanden sind.

> **Warning**
>
> Wenn Sie Ressourcen manuell entfernen, können Sie keine neue landing zone einrichten. Das ist nicht dasselbe wie die Außerbetriebnahme. Wenn Sie beabsichtigen, Ihre AWS

Control Tower Tower-Landezone landing zone zu nehmen, folgen Sie den Anweisungen unter, Außerbetriebnahme einer AWS Control Tower Tower-Landezone bevor Sie die in diesem Kapitel beschriebenen Maßnahmen ergreifen. Die Anweisungen in diesem Kapitel können Ihnen dabei helfen, Ressourcen zu bereinigen, die nach Abschluss der automatisierten Außerbetriebnahme noch vorhanden sind. Selbst wenn Sie alle Ressourcen Ihrer landing zone manuell löschen, ist dies nicht dasselbe wie die Außerbetriebnahme der landing zone, und es können unerwartete Kosten anfallen.

Wenn Sie ein Konto aus AWS Control Tower entfernen müssen, lesen Sie die folgenden Abschnitte, um ein Konto zu schließen:

- Verwaltung eines Kontos aufheben
- Schließen Sie ein in Account Factory erstelltes Konto

Muss ich außer Betrieb nehmen, anstatt zu löschen?

Wenn Sie nicht mehr beabsichtigen, AWS Control Tower für Ihr Unternehmen zu verwenden, oder wenn Sie eine größere Umschichtung Ihrer Unternehmensressourcen benötigen, möchten Sie möglicherweise die Ressourcen außer Betrieb nehmen, die bei der ursprünglichen Einrichtung Ihrer landing zone erstellt wurden.

- Nach Abschluss des Außerbetriebnahmevorgangs verbleiben einige Ressourcenartefakte wie Amazon S3 S3-Buckets und Amazon CloudWatch Logs-Protokollgruppen.
- Sie müssen die verbleibenden Ressourcen in Ihren Konten manuell bereinigen, bevor Sie eine weitere landing zone einrichten, um die Möglichkeit unerwarteter Gebühren zu vermeiden. Weitere Informationen finden Sie unter Ressourcen, die bei der Außerbetriebnahme nicht entfernt wurden.

Warning

Wir empfehlen Ihnen dringend, nur dann eine Außerbetriebnahme durchzuführen, wenn Sie beabsichtigen, Ihre landing zone nicht mehr zu nutzen. Dieser Vorgang kann nicht rückgängig gemacht werden.

Über das Entfernen von AWS Control Tower Tower-Ressourcen

Die einzelnen Verfahren in diesem Kapitel führen Sie durch die manuellen Methoden zum Entfernen von AWS Control Tower Tower-Ressourcen. Diese Verfahren können befolgt werden, wenn Sie eine bestimmte Ressource aus Ihrer landing zone löschen müssen.

Bevor Sie diese Verfahren durchführen können, müssen Sie, sofern nicht anders angegeben, AWS-Managementkonsole in der Heimatregion für Ihre landing zone angemeldet sein und Sie müssen als IAM-Benutzer oder Benutzer in IAM Identity Center mit Administratorberechtigungen für das Verwaltungskonto angemeldet sein, das Ihre landing zone enthält.

> **Warning**
>
> Dabei handelt es sich um destruktive Aktionen, die dazu führen können, dass die Steuerung Ihres AWS Control Tower Tower-Setups beeinträchtigt wird. Sie können nicht rückgängig gemacht werden.

Themen

- Löschen SCPs
- Löschen und Stapel StackSets
- Löschen Sie Amazon S3 S3-Buckets im Log Archive-Konto
- Ein Konto entfernen, ein Factory-Portfolio und ein Produkt
- Rollen und Richtlinien von AWS Control Tower entfernen
- Hilfe zu den Ressourcen von AWS Control Tower

Löschen SCPs

AWS Control Tower verwendet Service Control Policies (SCPs) für seine Kontrollen. In diesem Verfahren wird beschrieben, wie Sie die SCPs speziell mit AWS Control Tower verbundenen Dateien löschen.

Um zu löschen AWS Organizations SCPs

1. Öffnen Sie die Organisationskonsole unter https://console.aws.amazon.com/organizations/.
2. Öffnen Sie die Registerkarte Richtlinien und suchen Sie nach den Service Control-Richtlinien (SCPs), die das Präfix aws-guardrails- haben, und gehen Sie für jeden SCP wie folgt vor:

a. Trennen Sie die SCP von der zugewiesenen Organisationseinheit.

b. Löschen Sie die SCP.

Löschen und Stapel StackSets

AWS Control Tower verwendet StackSets und stapelt für die Bereitstellung AWS-Config-Regeln von Steuerungen in Ihrer landing zone. Die folgenden Verfahren zeigen, wie Sie diese Ressourcen löschen.

Um zu löschen CloudFormation StackSets

1. Öffnen Sie die CloudFormation Konsole unter https://console.aws.amazon.com/cloudformation.
2. Wählen Sie im linken Navigationsmenü. StackSets
3. Gehen Sie für jeden StackSet mit dem Präfix AWSControlTower wie folgt vor. Wenn Sie viele Konten in einem haben StackSet, kann dies einige Zeit dauern.

   a. Wählen Sie das spezifische StackSet aus der Tabelle im Dashboard aus. Dadurch wird die Eigenschaftenseite dafür geöffnet StackSet.

   b. Notieren Sie sich unten auf der Seite in der Tabelle Stacks das AWS Konto IDs für alle Konten in der Tabelle. Kopieren Sie die Liste mit allen Konten.

   c. Wählen Sie unter Aktionen die Option Stapel löschen aus. StackSet

   d. Wählen Sie unter Bereitstellungsoptionen festlegen unter Bereitstellungsorte die Option Stacks in Konten bereitstellen aus.

   e. Geben Sie in das Textfeld das AWS Konto, für das IDs Sie in Schritt 3.b einen Datensatz erstellt haben, durch Kommas getrennt ein. Beispiel: *123456789012*, *098765431098* usw.

   f. Wählen Sie unter Specify regions (Regionen angeben) die Option Add all (Alle auswählen) aus und behalten Sie für die restlichen Parameter auf der Seite die Standardwerte bei. Wählen Sie dann Next (Weiter) aus.

   g. Überprüfen Sie auf der Seite Review (Überprüfen) Ihre Auswahl und wählen Sie dann Delete stacks (Stacks löschen) aus.

   h. Auf der StackSet Eigenschaftenseite können Sie diesen Vorgang für Ihr anderes Gerät erneut ausführen. StackSets

4. Der Vorgang ist abgeschlossen, wenn die Datensätze in der Tabelle Stacks der verschiedenen StackSets Eigenschaftenseiten leer sind.

5. Wenn die Datensätze in der Stacks-Tabelle leer sind, wählen Sie Löschen. StackSet

Um Stapel zu löschen CloudFormation

1. Öffnen Sie die CloudFormation Konsole unter https://console.aws.amazon.com/cloudformation.
2. Suchen Sie im Stacks-Dashboard nach allen Stacks mit dem Präfix Tower. AWSControl
3. Gehen Sie für jeden Stack in der Tabelle wie folgt vor:
   a. Aktivieren Sie das Kontrollkästchen neben dem Namen des Stacks.
   b. Wählen Sie im Menü Actions (Aktionen) die Option Delete Stack (Stack löschen) aus.
   c. Stellen Sie sicher, dass die Informationen im Dialogfeld, das sich jetzt öffnet, korrekt sind. Wählen Sie dann Yes, Delete (Ja, löschen) aus.

Löschen Sie Amazon S3 S3-Buckets im Log Archive-Konto

Die folgenden Verfahren zeigen Ihnen, wie Sie sich als IAM Identity Center-Benutzer in der AWSControlTowerExecutionGruppe beim Protokollarchiv-Konto anmelden und anschließend die Amazon S3 S3-Buckets in Ihrem Protokollarchiv-Konto löschen.

So melden Sie sich mit den richtigen Berechtigungen bei Ihrem Protokollarchivkonto an

1. Öffnen Sie die Organisationskonsole unter https://console.aws.amazon.com/organizations/.
2. Suchen Sie auf der Registerkarte Accounts (Konten) das Konto Log archive (Protokollarchiv).
3. Notieren Sie im rechten Bereich, der jetzt geöffnet wird, die Nummer des Protokollarchivkontos.
4. Wählen Sie in der Navigationsleiste den Namen Ihres Kontos aus, um das Kontomenü zu öffnen.
5. Wählen Sie Switch Role.
6. Geben Sie auf der Seite, die jetzt geöffnet wird, im Feld Konto die Nummer des Protokollarchivkontos ein.
7. Geben Sie für Rolle den Wert ein AWSControlTowerExecution.
8. Nun wird das Feld Display Name (Anzeigename) ausgefüllt.
9. Wählen Sie unter Color (Farbe) eine Farbe aus.
10. Wählen Sie Switch Role.

So löschen Sie Amazon S3 S3-Buckets

1. Öffnen Sie die Amazon S3 S3-Konsole unter https://console.aws.amazon.com/s3/.
2. Suchen Sie nach Bucket-Namen, die aws-controltower enthalten.
3. Gehen Sie für jeden Bucket in der Tabelle wie folgt vor:
   a. Wählen Sie das Kontrollkästchen für den Bucket in der Tabelle aus.
   b. Wählen Sie Löschen aus.
   c. Stellen Sie sicher, dass die Informationen im Dialogfeld, das sich jetzt öffnet, korrekt sind. Geben Sie anschließend den Namen des zu bestätigenden Buckets ein und wählen Sie dann Confirm (Bestätigen) aus.

Ein Konto entfernen, ein Factory-Portfolio und ein Produkt

Das folgende Verfahren zeigt Ihnen, wie Sie sich als IAM Identity Center-Benutzer in der AWSServiceCatalogAdminsGruppe anmelden und anschließend Ihr Account Factory Factory-Portfolio und Ihre Produkte bereinigen.

So melden Sie sich mit den richtigen Berechtigungen bei Ihrem Verwaltungskonto an

1. Rufen Sie die URL Ihres Benutzerportals unter *directory-id* .awsapps.com/start auf
2. Suchen Sie unter AWS Konto nach dem Verwaltungskonto.
3. Wählen Sie unter Managementkonsole aus AWSServiceCatalogAdminFullAccess, um sich AWS-Managementkonsole mit dieser Rolle anzumelden.

Um Account Factory aufzuräumen

1. Öffnen Sie die Service Catalog-Konsole unter https://console.aws.amazon.com/servicecatalog/.
2. Klicken Sie im linken Navigationsmenü auf Portfolios list (Portfolioliste).
3. Suchen Sie in der Tabelle Lokale Portfolios nach einem Portfolio mit dem Namen AWS Control Tower Account Factory Portfolio.
4. Wählen Sie den Namen des Portfolios aus, um seine Detailseite aufzurufen.
5. Erweitern Sie den Abschnitt Einschränkungen auf der Seite und wählen Sie das Optionsfeld für die Einschränkung mit dem Produktnamen AWS Control Tower Account Factory.
6. Wählen Sie REMOVE CONSTRAINTS (Einschränkungen entfernen) aus.

7. Stellen Sie sicher, dass die Informationen im Dialogfeld, das sich jetzt öffnet, korrekt sind. Wählen Sie dann CONTINUE (Weiter) aus.
8. Wählen Sie im Bereich Produkte der Seite das Optionsfeld für das Produkt AWS Control Tower Account Factory aus.
9. Wählen Sie REMOVE PRODUCT (Produkt entfernen) aus.
10. Stellen Sie sicher, dass die Informationen im Dialogfeld, das sich jetzt öffnet, korrekt sind. Wählen Sie dann CONTINUE (Weiter) aus.
11. Erweitern Sie den Bereich Users, Groups, and Roles (Benutzer, Gruppen und Rollen) der Seite und wählen Sie die Kontrollkästchen für alle Einträge in dieser Tabelle aus.
12. Wählen Sie REMOVE USERS, GROUP OR ROLE (Benutzer, Gruppe oder Rolle entfernen) aus.
13. Stellen Sie sicher, dass die Informationen im Dialogfeld, das sich jetzt öffnet, korrekt sind. Wählen Sie dann CONTINUE (Weiter) aus.
14. Klicken Sie im linken Navigationsmenü auf Portfolios list (Portfolioliste).
15. Suchen Sie in der Tabelle Lokale Portfolios nach einem Portfolio mit dem Namen AWS Control Tower Account Factory Portfolio.
16. Wählen Sie das Optionsfeld für dieses Portfolio und dann die Option DELETE-PORTFOLIO (Portfolio löschen) aus.
17. Stellen Sie sicher, dass die Informationen im Dialogfeld, das sich jetzt öffnet, korrekt sind. Wählen Sie dann CONTINUE (Weiter) aus.
18. Klicken Sie im linken Navigationsmenü auf Product list (Produktliste).
19. Suchen Sie auf der Admin-Produktseite nach dem Produkt mit dem Namen AWS Control Tower Account Factory.
20. Wählen Sie das Produkt aus, um die Seite Admin product details (Details zu Administratorprodukten) zu öffnen.
21. Wählen Sie unter Actions (Aktionen) die Option Delete product (Produkt löschen) aus.
22. Stellen Sie sicher, dass die Informationen im Dialogfeld, das sich jetzt öffnet, korrekt sind. Wählen Sie dann CONTINUE (Weiter) aus.

Rollen und Richtlinien von AWS Control Tower entfernen

Diese Verfahren führen Sie durch die Bereinigung der Rollen und Richtlinien, die AWS Control Tower bei der Einrichtung Ihrer landing zone oder später erstellt hat.

Um die IAM Identity AWSService CatalogEndUserAccess Center-Rolle zu löschen

1. Öffnen Sie die AWS IAM Identity Center Konsole unter. https://console.aws.amazon.com/singlesignon/
2. Ändern Sie Ihre AWS Region in Ihre Heimatregion, die Region, in der Sie AWS Control Tower ursprünglich eingerichtet haben.
3. Wählen Sie im linken Navigationsmenü AWS Konten aus.
4. Wählen Sie den Link zu Ihrem Verwaltungskonto.
5. Wählen Sie das Drop-down-Menü für Berechtigungssätze aus AWSServiceCatalogEndUserAccess, wählen Sie und wählen Sie dann Entfernen aus.
6. Wählen Sie im linken Bereich AWS Konten aus.
7. Öffnen Sie die Registerkarte Permission sets (Berechtigungssätze).
8. Wählen Sie es aus AWSServiceCatalogEndUserAccessund löschen Sie es.

Um IAM-Rollen zu löschen

1. Öffnen Sie unter https://console.aws.amazon.com/iam/ die IAM-Konsole.
2. Klicken Sie im linken Navigationsmenü auf Roles (Rollen).
3. Suchen Sie in der Tabelle nach Rollen mit dem Namen AWSControlTower.
4. Gehen Sie für jede Rolle in der Tabelle wie folgt vor:
    a. Wählen Sie das Kontrollkästchen für die Rolle aus.
    b. Wählen Sie Delete role (Rolle löschen) aus.
    c. Stellen Sie sicher, dass die Informationen im Dialogfeld, das sich jetzt öffnet, korrekt sind. Wählen Sie dann Yes, delete (Ja, löschen) aus.

Um IAM-Richtlinien zu löschen

1. Öffnen Sie unter https://console.aws.amazon.com/iam/ die IAM-Konsole.
2. Klicken Sie im linken Navigationsmenü auf Policies (Richtlinien).
3. Suchen Sie in der Tabelle nach Richtlinien mit dem Namen AWSControlTower.
4. Gehen Sie für jede Richtlinie in der Tabelle wie folgt vor:
    a. Wählen Sie das Kontrollkästchen für die Richtlinie aus.

b. Wählen Sie Policy actions (Richtlinienaktionen) und dann im Dropdownmenü die Option Delete (Löschen) aus.

c. Stellen Sie sicher, dass die Informationen im Dialogfeld, das sich jetzt öffnet, korrekt sind. Wählen Sie dann Delete (Löschen) aus.

Hilfe zu den Ressourcen von AWS Control Tower

Wenn Sie beim Entfernen von AWS Control Tower Tower-Ressourcen auf Probleme stoßen, die Sie nicht lösen können, wenden Sie sich an den AWS Support.

Einrichtung nach der Außerbetriebnahme einer landing zone

Nachdem Sie Ihre Landing Zone außer Betrieb genommen haben, können Sie die Einrichtung erst dann wieder erfolgreich durchführen, wenn die manuelle Bereinigung abgeschlossen wurde. Außerdem können ohne manuelle Bereinigung dieser verbleibenden Ressourcen unerwartete Abrechnungskosten anfallen. Sie müssen sich mit diesen Aspekten befassen:

- Das AWS Control Tower-Managementkonto ist Teil der AWS Control Tower Root OU. Stellen Sie sicher, dass diese IAM-Rollen und IAM-Richtlinien aus dem Verwaltungskonto entfernt wurden:
  - Rollen:
    - `AWSControlTowerAdmin`
    - `AWSControlTowerCloudTrailRole`
    - `AWSControlTowerStackSetRole`
  - Richtlinien:
    - `AWSControlTowerAdminPolicy`
    - `AWSControlTowerCloudTrailRolePolicy`
    - `AWSControlTowerStackSetRolePolicy`
- Möglicherweise möchten Sie die bestehende IAM Identity Center-Konfiguration für AWS Control Tower löschen oder aktualisieren, bevor Sie erneut eine landing zone einrichten, aber es ist nicht erforderlich, dass Sie sie löschen.
- Möglicherweise möchten Sie die von AWS Control Tower erstellte VPC entfernen.

- Die Einrichtung schlägt fehl, wenn die für die Protokollierungs- oder Auditkonten angegebenen E-Mail-Adressen mit einem vorhandenen AWS Konto verknüpft sind. Sie können die AWS Konten schließen oder andere E-Mail-Adressen verwenden, um erneut eine landing zone einzurichten. Alternativ können Sie diese bestehenden gemeinsamen Konten mit der Funktion wiederverwenden, mit der Sie Ihre eigenen Protokollierungs- und Auditkonten verwenden können. Weitere Informationen finden Sie unter Überlegungen zur Verwendung vorhandener Sicherheits- oder Protokollkonten.
- Das Setup schlägt fehl, wenn Amazon S3 S3-Buckets mit den folgenden reservierten Namen bereits im Logging-Konto vorhanden sind:
  - `aws-controltower-logs-{accountId}-{region}` (wird für den Protokollierungsbucket verwendet).
  - `aws-controltower-s3-access-logs-{accountId}-{region}` (wird für den Bucket verwendet, mit dem Zugriffe protokolliert werden).

  Sie müssen diese Buckets entweder umbenennen oder entfernen oder ein anderes Konto für das Protokollierungskonto verwenden.
- Die Installation schlägt fehl, wenn das Verwaltungskonto die bestehende Protokollgruppe,`aws-controltower/CloudTrailLogs`, unter CloudWatch Logs hat. Sie müssen die Protokollgruppe entweder umbenennen oder entfernen.

Bevor Sie ein neues einrichten AWS-Region

Wenn Sie beabsichtigen, eine neue landing zone in einer neuen AWS Region einzurichten, gehen Sie wie folgt vor.

- Geben Sie den folgenden Befehl über die CLI ein:

```
aws organizations disable-aws-service-access --service-principal
 controltower.amazonaws.com
```

- Löschen Sie die verbleibende EventBridge Amazon-Regel, genanntAWSControlTowerManagedRule, aus den gemeinsamen Konten und Mitgliedskonten für alle kontrollierten Regionen.

Anleitungen

Dieses Kapitel enthält schrittweise Anleitungen, die Ihnen bei der Verwendung von AWS Control Tower helfen können.

Topics

- Exemplarische Vorgehensweise: Wechseln Sie von ALZ zum AWS Control Tower
- Exemplarische Vorgehensweise: Konfiguration des AWS Control Tower ohne VPC
- AWS Control Tower Tower-Ressourcen entfernen
- Exemplarische Vorgehensweise: Einrichten von Sicherheitsgruppen im AWS Control Tower mit AWS Firewall Manager
- Außerbetriebnahme einer AWS Control Tower Tower-Landezone

Exemplarische Vorgehensweise: Wechseln Sie von ALZ zum AWS Control Tower

Viele AWS Kunden haben die AWS Landing Zone-Lösung (ALZ) eingeführt, um eine sichere, konforme Umgebung mit mehreren Konten AWS einzurichten. Um den Verwaltungsaufwand für eine Landezone zu verringern, AWS wurde der verwaltete Service namens AWS Control Tower entwickelt.

Für ALZ sind keine zusätzlichen Funktionen geplant; es wird nur langfristig unterstützt. Daher empfehlen wir Ihnen, von ALZ auf den AWS Control Tower-Service umzusteigen. Der Blog, der in diesem Kapitel verlinkt ist, führt Sie durch die verschiedenen Überlegungen zu diesem Schritt und erklärt, wie Sie eine erfolgreiche Migration von ALZ zum AWS Control Tower planen können.

Blog: Migrieren Sie die AWS Landing Zone-Lösung zum AWS Control Tower

AWS Prescriptive Guidance bietet eine umfassendere Dokumentation, einschließlich der Schritte für den Übergang von ALZ zum AWS Control Tower. Im Wesentlichen aktivieren Sie die AWS Control Tower-Governance in Ihrer bestehenden Organisation, in der ALZ ausgeführt wird, basierend auf einer Reihe von Voraussetzungen. Weitere Informationen finden Sie unter Übergang von der AWS Landing Zone zum AWS Control Tower.

Exemplarische Vorgehensweise: Konfiguration des AWS Control Tower ohne VPC

In diesem Thema wird beschrieben, wie Sie Ihre AWS Control Tower-Konten ohne VPC konfigurieren.

Wenn für Ihren Workload keine VPC erforderlich ist, können Sie Folgendes tun:

- Sie können die virtuelle private Cloud (VPC) von AWS Control Tower löschen. Diese VPC wurde erstellt, als Sie Ihre Landing Zone eingerichtet haben.
- Sie können Ihre Account Factory-Einstellungen so ändern, dass neue AWS Control Tower-Konten ohne zugehörige VPC erstellt werden.

> **Important**
>
> Wenn Sie Account Factory-Konten mit aktivierten VPC-Internetzugangseinstellungen bereitstellen, überschreibt diese Account Factory-Einstellung die Einstellung Internetzugriff verbieten für eine Amazon VPC-Instance, die von einem Kunden verwaltet wird. Um zu verhindern, dass der Internetzugang für neu bereitgestellte Konten aktiviert wird, müssen Sie die Einstellung in Account Factory ändern.

Löschen Sie die AWS Control Tower VPC

Außerhalb des AWS Control Tower hat jeder AWS Kunde eine Standard-VPC, die Sie auf der Amazon Virtual Private Cloud (Amazon VPC) -Konsole unter einsehen können. https://console.aws.amazon.com/vpc/ Sie erkennen die Standard-VPC, da ihr Name immer das Wort (default) am Ende des Namens enthält.

Wenn Sie eine AWS Control Tower-Landezone einrichten, löscht AWS Control Tower Ihre AWS Standard-VPC und erstellt eine neue AWS Control Tower-Standard-VPC. Die neue VPC ist mit Ihrem AWS Control Tower-Verwaltungskonto verknüpft. Dieses Thema bezieht sich auf diese neue VPC als Control Tower-VPC.

Wenn Sie Ihre AWS Control Tower-VPC in der Amazon VPC-Konsole anzeigen, wird das Wort (Standard) am Ende des Namens nicht angezeigt. Wenn Sie mehr als eine VPC haben, müssen

Sie den zugewiesenen CIDR-Bereich verwenden, um die richtige AWS Control Tower-VPC zu identifizieren.

Sie können die AWS Control Tower VPC löschen, aber wenn Sie später eine VPC in AWS Control Tower benötigen, müssen Sie sie selbst erstellen.

Um die AWS Control Tower VPC zu löschen

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Suchen Sie in den Service Catalog-Optionen nach VPC **VPC** oder wählen Sie sie aus. Anschließend wird das VPC-Dashboard angezeigt.
3. Wählen Sie im Menü auf der linken Seite Your VPCs (Ihre VPCs) aus. Anschließend wird eine Liste aller Ihrer VPCs angezeigt.
4. Identifizieren Sie die AWS Control Tower VPC anhand ihres CIDR-Bereichs.
5. Wählen Sie die VPC aus, dann Actions (Aktionen) und anschließend Delete VPC (VPC löschen).

In jeder Region gibt es bereits eine AWS (Standard-) VPC für das AWS Control Tower-Managementkonto. Um den bewährten Sicherheitsmethoden zu folgen, empfiehlt es sich, wenn Sie die AWS Control Tower-VPC löschen, auch die AWS Standard-VPC, die dem Verwaltungskonto zugeordnet ist, aus allen Regionen zu löschen. AWS Um das Verwaltungskonto zu sichern, entfernen Sie daher die Standard-VPC aus jeder Region sowie die von Control Tower in Ihrer AWS Control Tower-Heimatregion erstellte VPC.

Bereinigen Sie optional die VPC-Ressource im Konto

Um die AWS Control Tower VPC-Ressource aus einem vorhandenen Konto zu bereinigen`aws-controltower-VPC`, können Sie optional die Stack-Instance aus dem entfernen AWS CloudFormation StackSet`AWSControlTowerBP-VPC-ACCOUNT-FACTORY-V1`, nachdem Sie sichergestellt haben, dass in der VPC keine vorhandenen Ressourcen oder Ressourcenabhängigkeiten vorhanden sind.

Erstellen Sie ein Konto in AWS Control Tower ohne VPC

Wenn für Ihre Endbenutzer-Workloads keine VPCs erforderlich sind, können Sie diese Methode verwenden, um Endbenutzerkonten einzurichten, für die nicht automatisch VPCs erstellt wurden.

Vom AWS Control Tower-Dashboard aus können Sie Ihre Netzwerkkonfigurationseinstellungen einsehen und bearbeiten. Nachdem Sie die Einstellungen so geändert haben, dass AWS Control

Tower-Konten ohne eine zugehörige VPC erstellt werden, werden alle neuen Konten ohne VPC erstellt, bis Sie die Einstellungen erneut ändern.

So konfigurieren Sie Account Factory für die Erstellung von Konten ohne VPCs

1. Öffnen Sie einen Webbrowser und navigieren Sie zur AWS Control Tower-Konsole unter https://console.aws.amazon.com/controltower.
2. Wählen Sie im Menü auf der linken Seite Account Factory aus.
3. Sie sehen dann die Account Factory-Seite mit dem Abschnitt Netzwerkkonfiguration.
4. Beachten Sie die aktuellen Einstellungen, wenn Sie sie später wiederherstellen möchten.
5. Wählen Sie die Schaltfläche Edit (Bearbeiten) im Abschnitt Network Configuration (Netzwerkkonfiguration) aus.
6. Wechseln Sie auf der Seite Edit account factory network configuration zum Abschnitt VPC Configuration options for new accounts.

   Sie können Option 1 oder Option 2 oder beide befolgen, um sicherzustellen, dass AWS Control Tower bei der Bereitstellung eines Kontos keine VPC erstellt.

   a. Option 1 — Subnetze entfernen

      - Schalten Sie den Internet-accessible Subnetz-Kippschalter aus.
      - Legen Sie den Wert Maximum number of private subnets (Maximale Anzahl an privaten Subnetzen) auf 0 fest.

   b. Option 2 — Entfernen AWS Regionen

      - Deaktivieren Sie jedes Kontrollkästchen in der Spalte Regions for VPC creation (Regionen für die VPC-Erstellung).
7. Wählen Sie Speichern.

Mögliche Fehler

Beachten Sie diese möglichen Fehler, die auftreten können, wenn Sie Ihre AWS Control Tower-VPC löschen oder Account Factory neu konfigurieren, um Konten ohne VPCs zu erstellen.

- Ihr vorhandenes Verwaltungskonto weist möglicherweise Abhängigkeiten oder Ressourcen in der AWS Control Tower VPC auf, was zu einem Fehler beim Löschen führen kann.

- Wenn Sie die Standard-CIDR beim Einrichten beibehalten, um neue Konten ohne VPC zu starten, schlägt Ihre Anfrage mit der Fehlermeldung fehl, dass die CIDR ungültig ist.

Exemplarische Vorgehensweise: Einrichten von Sicherheitsgruppen im AWS Control Tower mit AWS Firewall Manager

Das Video zeigt Ihnen, wie Sie den AWS Firewall Manager-Service verwenden, um Ihre Netzwerksicherheit für den AWS Control Tower zu verbessern. Sie können ein Sicherheitsadministratorkonto festlegen, das zum Einrichten von Sicherheitsgruppen aktiviert ist. Sie erfahren, wie Sie Sicherheitsrichtlinien konfigurieren und Sicherheitsregeln für Ihre AWS Control Tower-Organisationen durchsetzen können und wie Sie nicht konforme Ressourcen beheben können, indem Sie Richtlinien automatisch anwenden. Sie können die Sicherheitsgruppen einsehen, die für jedes Konto und jede Ressource (z. B. eine Amazon EC2-Instance) in Ihrer Organisation gültig sind.

Sie können eigene Firewall-Richtlinien erstellen oder Regeln von vertrauenswürdigen Anbietern abonnieren.

Richten Sie Sicherheitsgruppen ein mit AWS Firewall Manager

Dieses Video (8:02) beschreibt, wie Sie eine bessere Netzwerkinfrastruktursicherheit für Ihre Ressourcen und Workloads im AWS Control Tower einrichten. Wählen Sie zur besseren Ansicht das Symbol in der rechten unteren Ecke des Videos, um es in voller Bildschirmgröße anzuzeigen. Es stehen Untertitel zur Verfügung.

Videoanleitung zur Firewall-Setup im AWS Control Tower.

Weitere Informationen finden Sie in der Dokumentation zur Einrichtung von AWS WAF.

Fehlerbehebung

Wenn Sie bei der Verwendung von AWS Control Tower auf Probleme stoßen, können Sie die folgenden Informationen verwenden, um diese gemäß unseren Best Practices zu lösen. Wenn die Probleme, auf die Sie stoßen, nicht in den Rahmen der folgenden Informationen fallen oder wenn sie nach dem Versuch, sie zu lösen, weiterhin bestehen, wenden Sie sich an den AWS Support.

Themen

- Start der Landing Zone fehlgeschlagen
- Die Aktualisierung der Landing Zone ist mit einem KMS-Fehler fehlgeschlagen
- Die Landing Zone konnte nicht aktualisiert werden
- Fehler „Landezone ist nicht aktuell“
- New Account Provisioning Failed (Bereitstellung eines neuen Kontos fehlgeschlagen)
- Ein bestehendes Konto konnte nicht angemeldet werden
- Ein Account Factory-Konto konnte nicht aktualisiert werden
- Fehler: Erwähnter Fehler AWS Config
- Portfoliofehler bei AWS Control Tower Account Factory
- Fehler „Unzureichende Berechtigungen“ erhalten
- Detektivkontrollen wirken sich nicht auf Konten aus
- Der Fehler „Rate überschritten“ wurde zurückgegeben von AWS Organizations API
- Fehler beim Verschieben eines Account Factory Factory-Kontos direkt von einer AWS Control Tower Tower-Landezone in eine andere AWS Control Tower Tower-Landezone
- AWS Support

Start der Landing Zone fehlgeschlagen

Häufige Ursachen für Fehler beim Starten der Landing Zone:

- Fehlende Antwort auf eine Bestätigungs-E-Mail-Nachricht.
- CloudFormation StackSet Fehlschlag.

Bestätigungs-E-Mail-Nachrichten: Wenn Ihr Verwaltungskonto weniger als eine Stunde alt ist, können Probleme bei der Erstellung der zusätzlichen Konten auftreten.

Maßnahme

Wenn dieses Problem auftritt, überprüfen Sie Ihre E-Mail. Möglicherweise wurde Ihnen eine Bestätigungs-E-Mail gesendet, dass auf Antwort gewartet wird. Alternativ empfehlen wir, eine Stunde zu warten und es dann erneut zu versuchen. Wenn das Problem weiterhin besteht, wenden Sie sich an den AWS Support.

Fehlgeschlagen StackSets: Eine weitere mögliche Ursache für einen Fehlschlag beim Start der landing zone ist ein CloudFormation StackSet Fehlschlag. AWS Security Token Service (STS) - Regionen müssen im Verwaltungskonto für alle AWS Regionen aktiviert sein, die AWS Control Tower verwaltet, damit die Bereitstellung erfolgreich sein kann. Andernfalls können Stack-Sets nicht gestartet werden.

Maßnahme

Stellen Sie sicher, dass Sie alle erforderlichen AWS Security Token Service (STS) - Endpunktregionen aktivieren, bevor Sie AWS Control Tower starten.

Um ausgefallene Stack-Sets zu korrigieren und das Setup erneut zu versuchen

1. Navigieren Sie zur CloudFormation entsprechenden Konsole. AWS-Region
2. Bereinigen Sie den ausgefallenen Stack mit dem Namen AWSControlTowerBP-BASELINE-CLOUDTRAIL-MASTER.
3. Warten Sie, bis der Stack gelöscht wurde.
4. Kehren Sie zur AWS Control Tower Tower-Seite zurück.
5. Wählen Sie erneut landing zone einrichten aus.

Eine Liste der von AWS-Regionen AWS Control Tower unterstützten Programme finden Sie unterWie AWS Regionen arbeiten mit AWS Control Tower.

Die Aktualisierung der Landing Zone ist mit einem KMS-Fehler fehlgeschlagen

Die häufigste Ursache für Fehler bei der Aktualisierung der landing zone ist eine AWS KMS wichtige Richtlinie, die nicht gültig ist.

Häufige Gründe für eine ungültige KMS-Schlüsselrichtlinie:

- Tippfehler in der Richtlinie.
- Ich habe vergessen, die erforderliche Richtlinienerklärung hinzuzufügen.
- Falsche AWS Partition.
- Falsche Kontonummer in der Richtlinie.
- Ich habe vergessen, die Platzhalter in der Beispielrichtlinie zu entfernen.

Maßnahme

Überprüfen Sie Ihre Richtlinie, um nach diesen Fehlern zu suchen.

Weitere Informationen zu AWS KMS wichtigen Richtlinien finden Sie unter KMS-Schlüssel konfigurieren und Backup-Voraussetzungen.

Die Landing Zone konnte nicht aktualisiert werden

AWS Control Tower führt kein Rollback zu einer früheren landing zone Zone-Version durch, wenn ein Update fehlschlägt. Möglicherweise befindet sich Ihre landing zone in einem unbestimmten Zustand. Wenn ja, wenden Sie sich an den Support AWS .

Aktualisierungen der Landezone können aus verschiedenen Gründen fehlschlagen.

- Die Voraussetzungen wurden nicht erfüllt
- AWS Config In bestimmten Konten sind Ressourcen vorhanden
- Geschlossene Konten existieren

Die Voraussetzungen sind nicht erfüllt

Ein Landezone-Update muss dieselben Voraussetzungen erfüllen wie ein Landezonen-Setup. Lesen Sie sich vor dem Update die Prüfungen vor dem Start durch.

AWS Config Ressourcen sind in Sicherheits-OU-Konten vorhanden

Fügen Sie Ihren Audit - und Log-Archivkonten keine AWS Config Ressourcen hinzu. Die Aktualisierung der landing zone kann nicht abgeschlossen werden, wenn diese Ressourcen vorhanden sind. Diese Einschränkungen ähneln denen für die Registrierung eines Kontos oder die erstmalige Einrichtung einer landing zone. Weitere Informationen finden Sie unter Konten registrieren, für die bereits Ressourcen vorhanden AWS Config sind.

Geschlossene Konten sind vorhanden

Wenn sich ein Konto im Status „Geschlossen“ oder „Gesperrt“ befindet, kann ein Problem auftreten, wenn Sie versuchen, Ihre landing zone zu aktualisieren. Sie müssen das bereitgestellte Produkt auf jedem geschlossenen Konto löschen, bevor Sie ein Update für die landing zone durchführen.

Auf der Seite mit dem AWS Service Catalog bereitgestellten Produkt wird möglicherweise eine Fehlermeldung ähnlich der folgenden angezeigt:

```
AWSControlTowerExecution role can't be assumed on the account.
```

Häufiger Grund: Sie haben ein Konto gesperrt, ohne das bereitgestellte Produkt zu löschen.

Zu ergreifende Maßnahme: Wenn Sie diesen Fehler sehen, haben Sie zwei Möglichkeiten:

1. Wenden Sie sich an den AWS Support und öffnen Sie das Konto erneut, löschen Sie das bereitgestellte Produkt und schließen Sie das Konto erneut.
2. Entfernen Sie die Ressourcen aus dem StackSets , die aufgrund der Kontoschließung verwaist sind. (Diese Option ist nur verfügbar, wenn sie Instanzen mit dem Status Aktuell StackSets haben, die Sie nicht entfernen werden.)

Gehen Sie für jedes geschlossene Konto wie folgt vor StackSets, um die Ressourcen aus dem zu entfernen:

- Gehen Sie in jeden der AWS Control Tower StackSets und entfernen Sie die StackInstances aus jeder Region für das Konto, das geschlossen wurde.
- WICHTIG: Wählen Sie die Option Stack beibehalten, damit nur die Stack-Instances StackSet entfernt werden. StackSet kann vom geschlossenen Konto aus keine Rolle übernehmen. Daher schlägt es fehl, wenn versucht wird, die `AWSControlTowerExecution` Rolle anzunehmen, was zu der Fehlermeldung führt, die Sie erhalten haben.

Fehler „Landezone ist nicht aktuell“

Wenn Sie Ihre landing zone in letzter Zeit nicht aktualisiert haben, erhalten Sie möglicherweise eine Fehlermeldung, wenn Sie versuchen, wieder Zugriff auf AWS Control Tower zu erhalten. Möglicherweise wird eine Fehlermeldung ähnlich der folgenden angezeigt:

```
Unable to access Control Tower
```

Ihr Konto war zu lange inaktiv. Aufgrund von Inaktivität müssen Sie Ihre landing zone aktualisieren, um auf AWS Control Tower zugreifen zu können.

Ihr Landezone-Update schlägt jedoch möglicherweise fehl.

Zu ergreifende Schritte

Melden Sie sich beim Verwaltungskonto Ihrer Organisation an und melden Sie sich als Root-Benutzer an. Ihr IAM-Benutzer oder Benutzer im IAM Identity Center muss über AWS Control Tower Tower-Administratorrechte verfügen und Teil der AWSControlTowerAdminsGruppe sein. Versuchen Sie dann erneut, das Update durchzuführen.

New Account Provisioning Failed (Bereitstellung eines neuen Kontos fehlgeschlagen)

Wenn dieses Problem auftritt, überprüfen Sie diese häufigen Ursachen.

Wenn Sie das Formular zur Kontobereitstellung ausgefüllt haben, verfügen Sie möglicherweise über Folgendes:

- angegebene TagOptions,
- aktivierte SNS-Benachrichtigungen,
- aktivierte bereitgestellte Produktbenachrichtigungen.

Versuchen Sie erneut, Ihr Konto bereitzustellen, ohne irgendwelche dieser Optionen anzugeben. Weitere Informationen finden Sie unter Stellen Sie Konten in der Service Catalog-Konsole mit Account Factory bereit.

Andere häufige Fehlerursachen:

- Wenn Sie einen bereitgestellten Produktplan erstellt haben (um Ressourcenänderungen anzuzeigen), behält Ihre Kontobereitstellung möglicherweise unbegrenzt lange den Status In progress (In Bearbeitung) bei.
- Die Erstellung eines neuen Kontos in Account Factory schlägt fehl, während andere AWS Control Tower Tower-Konfigurationsänderungen im Gange sind. Während beispielsweise ein Prozess zum Hinzufügen eines Steuerelements zu einer Organisationseinheit ausgeführt wird, zeigt Account Factory eine Fehlermeldung an, wenn Sie versuchen, ein Konto bereitzustellen.

Um den Status einer vorherigen Aktion in AWS Control Tower zu überprüfen

- Navigieren Sie zu AWS CloudFormation > StackSets
- Überprüfen Sie jedes Stack-Set, das sich auf AWS Control Tower bezieht (Präfix: "AWSControlTower„)
- Suchen Sie nach CloudFormation StackSets Vorgängen, die noch laufen.

Wenn die Kontobereitstellung länger als eine Stunde dauert, beenden Sie den Bereitstellungsprozess am besten und versuchen Sie es erneut.

Ein bestehendes Konto konnte nicht angemeldet werden

Wenn Sie einmal versuchen, ein vorhandenes AWS Konto zu registrieren, und diese Registrierung schlägt fehl, wenn Sie es ein zweites Mal versuchen, weist Sie die Fehlermeldung möglicherweise darauf hin, dass das Stack-Set vorhanden ist. Um fortzufahren, müssen Sie das bereitgestellte Produkt in Account Factory entfernen.

Wenn der Grund für den ersten Anmeldungsfehler darin bestand, dass Sie vergessen haben, die `AWSControlTowerExecution`-Rolle in dem Konto im Voraus zu erstellen, fordert die Fehlermeldung Sie korrekterweise auf, die Rolle zu erstellen. Wenn Sie jedoch versuchen, die Rolle zu erstellen, erhalten Sie wahrscheinlich eine weitere Fehlermeldung, die besagt, dass AWS Control Tower die Rolle nicht erstellen konnte. Dieser Fehler tritt auf, weil der Prozess teilweise abgeschlossen wurde.

In diesem Fall müssen Sie zwei Wiederherstellungsschritte durchführen, bevor Sie mit der Anmeldung Ihres bestehenden Kontos fortfahren können. Zunächst müssen Sie das von Account Factory bereitgestellte Produkt über die AWS Service Catalog Konsole kündigen. Als Nächstes müssen Sie die AWS Organizations Konsole verwenden, um das Konto manuell aus der Organisationseinheit und zurück in das Stammverzeichnis zu verschieben. Danach erstellen Sie die `AWSControlTowerExecution`-Rolle in dem Konto und füllen dann das Formular Enroll account (Konto anmelden) erneut aus.

Eine weitere mögliche Ursache für einen Registrierungsfehler ist, dass das Konto über vorhandene AWS Konfigurationsressourcen verfügt. In diesem Fall finden Sie unter Registrieren von Konten mit vorhandenen AWS Config Ressourcen Anweisungen, wie Sie Ihre vorhandenen Ressourcen ändern können.

Ein Account Factory-Konto konnte nicht aktualisiert werden

Wenn sich ein Konto in einem inkonsistenten Zustand befindet, kann es nicht erfolgreich über Account Factory oder AWS Service Catalog aktualisiert werden.

Fall 1: Möglicherweise wird eine Fehlermeldung ähnlich der folgenden angezeigt:

```
AWS Control Tower could not baseline VPC in the managed account because of existing resource dependencies.
```

Häufiger Grund: AWS Control Tower entfernt bei der ersten Bereitstellung immer die AWS Standard-VPC. Um eine AWS Standard-VPC in einem Konto zu haben, müssen Sie sie nach der Kontoerstellung hinzufügen. AWS Control Tower verfügt über eine eigene Standard-VPC, die die AWS Standard-VPC ersetzt, es sei denn, Sie richten Account Factory so ein, wie es Ihnen in der Anleitung gezeigt wird — sodass AWS Control Tower überhaupt keine VPC bereitstellt. Dann hat das Konto keine VPC. Sie müssten die AWS Standard-VPC erneut hinzufügen, wenn Sie diese verwenden möchten.

AWS Control Tower unterstützt die AWS Standard-VPC jedoch nicht. Die Bereitstellung eines Kontos führt dazu, dass das Konto in einen `Tainted`-Status wechselt. Wenn es sich in diesem Status befindet, können Sie das Konto nicht aktualisieren. AWS Service Catalog

Maßnahme: Sie müssen die hinzugefügte Standard-VPC löschen, dann können Sie das Konto aktualisieren.

> **Note**
>
> Dieser `Tainted` Status verursacht ein Folgeproblem: Ein Konto, das nicht aktualisiert wird, verhindert möglicherweise die Aktivierung von Steuerelementen in der Organisationseinheit, zu der es gehört.

Fall 2: Möglicherweise wird eine Fehlermeldung ähnlich der folgenden angezeigt:

```
AWS Control Tower detects that your enrolled account has been moved to a new organizational unit.
```

Häufiger Grund: Sie haben versucht, ein Konto von einer registrierten Organisationseinheit in eine andere zu verschieben, aber die alten AWS Config-Regeln bleiben bestehen. Das Konto befindet sich in einem inkonsistenten Zustand.

Zu ergreifende Maßnahmen:

Falls die Kontoverschiebung beabsichtigt war:

- Kündigen Sie das Konto im Service Catalog.
- Registrieren Sie es erneut.
- Context/impact: Die bereitgestellten AWS Konfigurationsregeln stimmen nicht mit der Konfiguration überein, die von der Ziel-OU vorgegeben wird.
- AWS Die Konfigurationsregeln können von der vorherigen Organisationseinheit übernommen werden, was zu unbeabsichtigten Ausgaben führen kann.
- Versuche, das Konto erneut zu registrieren oder zu aktualisieren, schlagen aufgrund von Konflikten bei der Benennung von Ressourcen fehl.

Falls die Kontoverschiebung unbeabsichtigt war:

- Setze das Konto auf seine ursprüngliche Organisationseinheit zurück.
- Aktualisieren Sie das Konto aus dem Service Catalog.
- Geben Sie in den Startparametern die Organisationseinheit ein, in der sich das Konto ursprünglich befand.
- Context/impact: Wenn das Konto nicht in seine ursprüngliche Organisationseinheit zurückversetzt wird, entspricht sein Status nicht den Kontrollen, die von der neuen Organisationseinheit, in der es sich befindet, vorgegeben werden.
- Die Aktualisierung eines Kontos ist keine gültige Abhilfemaßnahme, da dadurch die AWS Config Regeln der vorherigen Organisationseinheit nicht gelöscht werden.

Fehler: Erwähnter Fehler AWS Config

Wenn in einer von AWS Control Tower unterstützten AWS Region aktiviert AWS Config ist, erhalten Sie möglicherweise eine Fehlermeldung, weil eine Vorabprüfung fehlgeschlagen ist. Die Meldung scheint das Problem möglicherweise nicht angemessen zu erklären, was auf ein grundlegendes Verhalten von AWS Config zurückzuführen ist.

Möglicherweise erhalten Sie eine Fehlermeldung, ähnlich einer der folgenden:

- `AWS Control Tower cannot create an AWS Config delivery channel because one already exists. To continue, delete the existing delivery channel and try again .`
- `AWS Control Tower cannot create an AWS Config configuration recorder because one already exists. To continue, delete the existing delivery channel and try again .`

Häufige Ursache: Wenn der AWS Config Dienst für ein AWS Konto aktiviert ist, erstellt er einen Konfigurationsrekorder und einen Bereitstellungskanal mit einer Standardbenennung. Wenn Sie den AWS Config Dienst über die Konsole deaktivieren, werden weder der Konfigurationsrekorder noch der Bereitstellungskanal gelöscht. Sie müssen sie über die CLI löschen oder für die Verwendung in AWS Control Tower ändern. Wenn der AWS Config Service in einer der von AWS Control Tower unterstützten Regionen aktiviert ist, kann dies zu diesem Fehler führen.

Wenn das Konto bereits über AWS Config-Ressourcen verfügt, finden Sie unter Konten mit vorhandenen AWS Config Ressourcen registrieren Anweisungen, wie Sie Ihre vorhandenen Ressourcen ändern können.

Zu ergreifende Aktion: Löschen Sie den Konfigurationsrecorder und den Bereitstellungskanal in allen unterstützten Regionen. Das Deaktivieren von AWS Config reicht nicht aus, der Konfigurationsrekorder und der Lieferkanal müssen über die CLI gelöscht werden. Nachdem Sie den Konfigurationsrekorder und den Lieferkanal aus der CLI gelöscht haben, können Sie erneut versuchen, AWS Control Tower zu starten und das Konto zu registrieren.

Wenn Sie gerade dabei sind, ein bereitgestelltes Produkt bereitzustellen, müssen Sie das bereitgestellte Produkt löschen, bevor Sie es erneut versuchen. Andernfalls wird möglicherweise eine Fehlermeldung ähnlich der folgenden angezeigt:

- `An error occurred` **`(InvalidParametersException)`** `when calling the` **`ProvisionProduct`** `operation: A stack named` *`Stackname`* `already exists.`

*`Stackname`*Gibt in der Nachricht den Namen des Stacks an.

Im Folgenden finden Sie einige AWS Config CLI-Beispielbefehle, mit denen Sie den Status Ihres Konfigurationsrekorders und Ihres Bereitstellungskanals ermitteln können.

Befehle anzeigen:

- `aws configservice describe-delivery-channels`
- `aws configservice describe-delivery-channel-status`
- `aws configservice describe-configuration-recorders`
- `The normal response is something like "name": "default"`

Befehle löschen:

- `aws configservice stop-configuration-recorder --configuration-recorder-name NAME-FROM-DESCRIBE-OUTPUT`
- `aws configservice delete-delivery-channel --delivery-channel-name NAME-FROM-DESCRIBE-OUTPUT`
- `aws configservice delete-configuration-recorder --configuration-recorder-name NAME-FROM-DESCRIBE-OUTPUT`

Weitere Informationen finden Sie im AWS Config Dokumentation

- Den Configuration Recorder (AWS CLI) verwalten
- Verwalten des Übermittlungskanals

Portfoliofehler bei AWS Control Tower Account Factory

Wenn Sie versuchen, ein Konto zu erstellen, zu registrieren oder zu aktualisieren, wird möglicherweise eine der folgenden Fehlermeldungen angezeigt:

```
Your AWS IAM identity does not have access to the AWS Control Tower Account Factory portfolio in AWS Service Catalog. To resolve this, an administrator must associate your AWS IAM identity with the portfolio.
```

oder

```
No launch paths found for resource: prod-xxxx
```

Häufige Ursachen:

- Möglicherweise sind Sie als Root angemeldet. AWS Control Tower unterstützt das Erstellen von Konten nicht, wenn Sie als Root-Benutzer angemeldet sind.
- Ihr IAM Identity Center-Benutzer wurde nicht zur entsprechenden Berechtigungsgruppe hinzugefügt. Möglicherweise müssen Sie Ihren IAM Identity Center-Benutzer zu einer dieser Berechtigungsgruppen hinzufügen: AWSAccountFactory(für Endbenutzerzugriff) oder AWSServiceCatalogAdmins(für Administratorzugriff).
- Wenn Sie als IAM-Benutzer authentifiziert sind, müssen Sie ihn dem AWS Service Catalog Portfolio hinzufügen, damit er über die richtigen Berechtigungen verfügt.
- Dieses Problem tritt auch auf, wenn Sie über die richtigen Berechtigungen verfügen, aber ein AWS Control Tower Tower-Drift erkannt wird und eine Drift-Reparatur erforderlich ist. Um die meisten Arten von Drift zu reparieren, wählen Sie auf der Seite mit den Landingzone-Einstellungen die Option Zurücksetzen.

Fehler „Unzureichende Berechtigungen“ erhalten

Es ist möglich, dass Ihr Konto nicht über die erforderlichen Berechtigungen verfügt, um bestimmte Arbeiten auszuführen AWS Organizations. Wenn der folgende Fehler auftritt, überprüfen Sie alle Berechtigungsbereiche, z. B. IAM- oder IAM Identity Center-Berechtigungen, um sicherzustellen, dass Ihre Erlaubnis nicht von diesen Orten aus verweigert wird:

```
You have insufficient permissions to perform AWS Organizations API actions.
```

Wenn Sie der Meinung sind, dass Ihre Arbeit die Aktion erfordert, die Sie versuchen, und Sie keine relevante Einschränkung finden können, wenden Sie sich an Ihren Systemadministrator oder AWS Support.

Detektivkontrollen wirken sich nicht auf Konten aus

Wenn Sie Ihre AWS Control Tower-Bereitstellung vor Kurzem auf eine neue AWS Region ausgeweitet haben, werden neu eingeführte Detektivkontrollen für neue Konten, die Sie in einer Region erstellen, erst wirksam, wenn die einzelnen Konten innerhalb der von AWS Control Tower verwalteten Organisationseinheiten aktualisiert wurden. Bestehende detektivische Kontrollen für bestehende Konten sind weiterhin in Kraft.

Wenn Sie versuchen, eine Detektivkontrolle zu aktivieren, bevor Sie Ihre Konten aktualisieren, wird möglicherweise eine Fehlermeldung ähnlich der folgenden angezeigt:

```
AWS Control Tower can't enable the selected control on this OU. AWS Control Tower cannot apply the control on the OU ou-xxx-xxxxxxxx, because child accounts have dependencies that are missing. Update all child accounts under the OU, then try again.
```

Zu ergreifende Maßnahme: Aktualisieren der Konten.

Informationen zum Aktualisieren Ihrer Konten von der AWS Control Tower Tower-Konsole aus finden Sie unterWann sollten die Organisationseinheiten und Konten von AWS Control Tower aktualisiert werden.

Um mehrere einzelne Konten programmgesteuert zu aktualisieren, können Sie die APIs von AWS Service Catalog und die AWS CLI verwenden, um die Updates zu automatisieren. Weitere Informationen über die Vorgehensweise beim Aktualisierungsvorgang finden Sie in diesem Video-Anleitung. Sie können die im Video UpdateProvisionedProductgezeigte ProvisionProductAPI durch die API ersetzen.

Wenn Sie weitere Probleme mit der Aktivierung von Detective Controls für Ihre Konten haben, wenden Sie sich an den AWS Support.

Der Fehler „Rate überschritten“ wurde zurückgegeben von AWS Organizations API

Mögliche Ursache

Ihr Workload lief, während AWS Control Tower täglich einen Scan durchführte, um zu überprüfen, ob sich Ihre SCPs verändert haben.

Folgende Schritte sind zu beachten

Wenn Sie auf eine API-Drosselung oder einen `rate exceeded` Fehler stoßen, versuchen Sie es mit diesen Schritten:

- Führen Sie Ihre Workloads zu einem anderen Zeitpunkt aus. (Im Zeitplan für SCP-Invarianzscans von AWS Control Tower nach Regionen finden Sie Informationen darüber, wann AWS Control Tower seine Audit-Scans durchführt.)

- Wenn Sie die APIs direkt über HTTP aufrufen: Verwenden Sie das AWS SDK, das fehlgeschlagene Aktionen automatisch wiederholt
- Beantragen Sie eine Limiterhöhung über Service Quotas und AWS Support

Ein Beispiel für Anweisungen zur Fehlerbehebung bei API-Drosselung in Elastic Beanstalk finden Sie hier: `https://aws.amazon.com/premiumsupport/knowledge-center/elastic-beanstalk-api-throttling-errors/`

Fehler beim Verschieben eines Account Factory Factory-Kontos direkt von einer AWS Control Tower Tower-Landezone in eine andere AWS Control Tower Tower-Landezone

> **Warning**
>
> Diese Vorgehensweise erfüllt nicht die Voraussetzung für die Registrierung eines berechtigten Kontos, da berechtigte Konten Teil derselben gesamten AWS-Organisation sein müssen und jede Organisation nur eine landing zone haben darf. Wenn Sie versucht haben, diese Aktion durchzuführen und Sie feststellen, dass Sie mehrere Fehlermeldungen erhalten, finden Sie hier einige Informationen, die hilfreich sein könnten.

Um ein Konto, das Sie über Account Factory bereitgestellt haben, in eine andere landing zone zu verschieben, die von AWS Control Tower verwaltet wird, und zwar unter einem anderen Verwaltungskonto, müssen Sie alle IAM-Rollen und die mit diesem Konto verknüpften Stacks aus der ursprünglichen Organisationseinheit entfernen. Entfernen Sie diese Ressourcen aus jeder Region, in der das Konto bereitgestellt wird.

> **Note**
>
> Die beste Methode zum Entfernen der Ressourcen besteht darin, die Bereitstellung des Kontos in seiner ursprünglichen Organisationseinheit aufzuheben, bevor Sie versuchen, es zu verschieben.

Wenn Sie die Ressourcen nicht entfernen, schlägt die Registrierung in der neuen Organisationseinheit fehl, was ziemlich spektakulär ist. Möglicherweise werden eine oder mehrere

Fehlermeldungen angezeigt, und Sie erhalten weiterhin ähnliche Fehlermeldungen, bis die verbleibenden Rollen und Stacks aus allen Regionen, in denen das Konto bereitgestellt wurde, entfernt wurden.

Jedes Mal, wenn Sie eine Fehlermeldung erhalten, müssen Sie das Konto aus der neuen Organisationseinheit entfernen, die alte Ressource löschen, die Gegenstand der Fehlermeldung ist, und dann versuchen, das Konto wieder in die neue Organisationseinheit zu verschieben. Dieser Vorgang des Entfernens und Löschens muss für jede verbleibende Ressource und für jede Region, in der das Konto bereitgestellt wurde, wiederholt werden, möglicherweise 10 oder 20 Mal. Diese wiederholten Fehler treten auf, weil das Konto in einer Organisationseinheit mit einem SCP bereitgestellt wurde, der das Löschen der IAM-Rolle verhindert. Sie können den Wiederherstellungsprozess verkürzen, indem Sie alle Ressourcen des Kontos löschen, bevor Sie es erneut versuchen.

Die folgenden Beispiele stellen die Arten von Fehlermeldungen dar, die Sie möglicherweise erhalten, wenn ungelöschte Rollen und Stacks bestehen bleiben. Höchstwahrscheinlich wird Ihnen bei jedem Versuch, das Konto zu registrieren, jeweils eine dieser Meldungen angezeigt, solange die alten Ressourcen noch verfügbar sind.

Die Werte der Ressourcen-ID-Zeichenfolgen wurden für die Beispiele geändert. Ihre Werte werden in einer Fehlermeldung, die Sie möglicherweise erhalten, nicht identisch sein. Möglicherweise wird eine Meldung angezeigt, die den folgenden Beispielen ähnelt:

- `AWS Control Tower cannot create the IAM role aws-controltower-AdministratorExecutionRole because the role already exists. To continue, delete the existing IAM role and try again.`
- `AWS Control Tower cannot create the IAM role aws-controltower-ConfigRecorderRole because the role already exists. To continue, delete the existing IAM role and try again.`
- `AWS Control Tower cannot create the IAM role aws-controltower-ForwardSnsNotificationRole because the role already exists. To continue, delete the existing IAM role and try again.`

Möglicherweise wird Ihnen auch eine Fehlermeldung über einen Stack-Set-Fehler angezeigt, die der folgenden ähnelt:

```
"Error\":\"StackSetFailState\",
```

```
\"Cause\":\"StackSetOperation on AWSControlTowerBP-BASELINE-CLOUDWATCH
with id 8aXXXXf5-e0XX-4XXa-bc4XX-dXXXXXee31
has reached SUCCEEDED state but has 1 NON-CURRENT stack instances;
here is the summary :{ StackSet Id:
AWSControlTowerBP-BASELINE-CLOUDWATCH:40XXXbf2-Xead-46a1-XXXa-eXXXXecb2ee2,
Stack instance Id:
arn:aws:cloudformation:eu-west-1:1X23456789XX:
            stack/StackSet-AWSControlTowerBP-BASELINE-CLOUDWATCH-4feXXXXXX-ecXX-XXc6-
bXXX-4ae678/4feXXXXXX-ecX-4ae123458,
Status: OUTDATED,
Status Reason: ResourceLogicalId:ForwardSnsNotification,
ResourceType:AWS::Lambda::Function,
ResourceStatusReason:aws-controltower-NotificationForwarder already exists in stack
arn:aws:cloudformation:eu-west-1:1X23456789XX:
            stack/StackSet-AWSControlTowerBP-BASELINE-CLOUDWATCH-4feXXXXXX-ecXX-XXc6-
bXXX-4ae678/4feXXXXXX-ecX-4ae123458.
```

Nachdem alle verbleibenden Ressourcen aus der ersten Organisationseinheit entfernt wurden, können Sie das Konto erfolgreich in die neue Organisationseinheit einladen, bereitstellen oder registrieren.

AWS Support

Wenn Sie Ihre vorhandenen Mitgliedskonten in einen anderen Supportplan verschieben möchten, können Sie sich bei jedem Konto mit den Anmeldeinformationen des Stammkontos anmelden, Pläne vergleichen und die gewünschte Supportstufe festlegen.

Es wird empfohlen, dass Sie die MFA- und Kontosicherheitskontakte aktualisieren, wenn Sie Änderungen an Ihrem Supportplan vornehmen.

Arten von Basislinien

Eine Baseline in AWS Control Tower ist eine Gruppe von Ressourcen und spezifischen Konfigurationen, die Sie auf ein Ziel anwenden können. Das gängigste Basisziel kann eine Organisationseinheit (OU) sein. Sie können beispielsweise eine Baseline mit einer als Ziel ausgewählten Organisationseinheit aktivieren, um diese Organisationseinheit bei AWS Control Tower zu registrieren.

Während der Einrichtung der landing zone aktiviert AWS Control Tower automatisch bestimmte Baselines für Service-Integrationskonten. Es aktiviert und aktualisiert diese Baselines auf der Grundlage Ihrer Landingzone-Einstellungen und -Konfigurationen. AWS Control Tower erstellt die Ressourcen und stellt sie auf dem Ziel bereit, wie es die Baseline vorgibt.

Wenn Sie eine Baseline auf einem Ziel aktivieren, wird die Baseline als AWS-Ressource dargestellt, die als `EnabledBaseline` Ressource bezeichnet wird.

AWS Control Tower umfasst zwei allgemeine Arten von Baselines:

- Baselines, die auf einer OU aktiviert werden können.
- Baselines, die während der Einrichtung der landing zone auf Serviceintegrationskonten aktiviert werden können.

Basistypen, die auf OU-Ebene gelten

> **Note**
>
> Nur Baselines, die auf OU-Ebene gelten, können direkt mit der `EnableBaseline` API aktiviert werden.

- Name (Name: `AWSControlTowerBaseline`

  Beschreibung: Diese Baseline richtet Ressourcen und Kontrollen für Mitgliedskonten innerhalb der Ziel-OU ein, die für die Compliance-Überwachung, Prüfung, Sicherheitsüberwachung und optional für die Zugriffsverwaltung erforderlich sind. Diese Baseline wird aktiviert, wenn Sie eine Organisationseinheit in AWS Control Tower registrieren.

Voraussetzung: Die AWS Config-Integration muss in der AWS Control Tower Tower-Landing landing zone aktiviert sein.

Überlegung: Diese Basislinie behält die Einstellungen der landing zone Region Deny Control bei. Mit anderen Worten, wenn eine Region auf Landing-Zone-Ebene nicht zulässig ist, ist diese Region für diese Organisationseinheit nicht zulässig, wenn Sie die `EnableBaseline` API aufrufen, um eine OU zu registrieren.

> **Note**
>
> Die OU-level Region Deny Control hat keine Möglichkeit, Regionen zuzulassen, die die landing zone Region Deny Control nicht zulässt.

Weitere Informationen finden Sie in der AWS Organizations Dokumentation unter So arbeiten SCPs mit Deny.

Empfehlung: Wir empfehlen Ihnen, die Regionen zu überprüfen, in denen Ihre Ziel-OU möglicherweise Workloads ausführt, und die Ergebnisse mit der landing zone Region Deny Control zu vergleichen, bevor Sie die `EnableBaseline` API für die Organisationseinheit aufrufen, da Sie sonst den Zugriff auf Ressourcen in bestimmten Regionen verlieren könnten.

- Name (Name: `ConfigBaseline`

  Beschreibung: Diese Baseline richtet AWS Config-bezogene Ressourcen für Mitgliedskonten innerhalb der Ziel-OU ein, die für die Aktivierung von Detective Controls erforderlich sind. Die eingerichteten Ressourcen sind eine Teilmenge der Ressourcen von. AWSControlTowerBaseline

  Voraussetzung: Die AWS Config-Integration muss in der AWS Control Tower Tower-Landing landing zone aktiviert sein.

  Überlegung: Diese Baseline enthält nicht die Einstellungen der landing zone Region Deny Control. Die Steuerung der Regionsverweigerung wird im Rahmen der Aktivierung nicht aktiviert ConfigBaseline.

  Einschränkung: AWSControlTowerBaseline und ConfigBaseline kann nicht auf derselben Organisationseinheit aktiviert werden. In einer Organisationseinheit ist nur eine davon zulässig.

> **⚠ ConfigBaseline Status „Nicht aktiviert“**
>
> Wenn Ihre Organisationseinheit `AWSControlTowerBaseline` aktiviert ist, wird der `ConfigBaseline` Status „Nicht aktiviert“ angezeigt. Dieses Verhalten wird erwartet. `AWSControlTowerBaseline`beinhaltet AWS Config Funktionalität. Sie müssen die Aktivierung nicht separat für Organisationseinheiten `ConfigBaseline` durchführen, die dies bereits getan haben`AWSControlTowerBaseline`.

- Name (Name: `BackupBaseline`

  Beschreibung: Diese Baseline richtet Ressourcen und Kontrollen für Mitgliedskonten innerhalb der Ziel-OU ein. Diese sind erforderlich, damit die Integration mit Ihre gesamte AWS-Services Datensicherung automatisieren und Ihr Backup-Policy-Management zentralisieren AWS Backup kann.

  Voraussetzungen:

  - Die AWS-Backup-Integration muss in der AWS Control Tower Tower-Landing landing zone aktiviert sein.
  - Die AWS Config-Integration muss in der AWS Control Tower Tower-Landezone aktiviert sein.
  - `AWSControlTowerBaseline`muss auf der Ziel-OU aktiviert sein.

  Überlegung: Bevor Sie das `BackupBaseline` auf einer Ziel-OU aktivieren, stellen Sie sicher, dass das auf der Ziel-OU aktiviert `AWSControlTowerBaseline` ist. Das heißt, die Ziel-OU muss in AWS Control Tower registriert sein.

  - Sie können wählen, ob die Aktivierung AWS Backup während der Erstellung Ihrer AWS Control Tower Tower-Landezone oder während eines Landing-Zone-Aktualisierungsprozesses erfolgen soll.
  - Das `BackupBaseline` ist mit den landing zone Zone-Versionen 3.1 und höher kompatibel.
  - Das `BackupBaseline` wird nicht auf das Verwaltungskonto angewendet.

Basistypen, die bei der Einrichtung der landing zone für Serviceintegrationskonten gelten

AWS Control Tower aktiviert im Rahmen der Einrichtung und Aktualisierung der landing zone bestimmte Basiswerte für Service-Integrationskonten. Die Basislinien für Ihre landing zone können

sich ändern, wenn Sie Ihre Landezoneneinstellungen ändern. Wenn Sie sich beispielsweise für IAM Identity Center entscheiden, kann AWS Control Tower die neueste Version der `IdentityCenterBaseline` Baseline in Ihrer landing zone aktivieren.

Sie können die aktivierten Baselines für Ihre landing zone mit dem `ListEnabledBaselines` API-Aufruf anzeigen.

> **Note**
>
> Ab Landing Zone Version 4.0 AuditBaseline wird der durch zwei unterschiedliche Baselines ersetzt: und. `CentralSecurityRolesBaseline` `CentralConfigBaseline`

- Name (Name: `CentralConfigBaseline`

  Beschreibung: Richtet mithilfe von AWS Config zentrale Ressourcen für die Überwachung und Prüfung der Einhaltung von Vorschriften in Ihrem Unternehmen ein.
- Name (Name: `CentralSecurityRolesBaseline`

  Beschreibung: Richtet zentrale Ressourcen für die Sicherheitsüberwachung in Ihrem Unternehmen ein.
- Name (Name: `AuditBaseline`

  Beschreibung: Richtet Ressourcen zur Überwachung der Sicherheit und Einhaltung von Vorschriften für Konten in Ihrer Organisation ein.
- Name (Name: `LogArchiveBaseline`

  Beschreibung: Richtet ein zentrales Repository für Protokolle von API-Aktivitäten und Ressourcenkonfigurationen von Konten in Ihrer Organisation ein.
- Name (Name: `IdentityCenterBaseline`

  Beschreibung: Richtet gemeinsam genutzte Ressourcen für IAM Identity Center ein und bereitet die Einrichtung des `AWSControlTowerBaseline` Identity Center-Zugriffs für Konten vor.

  Überlegung: Diese Baseline funktioniert nur, wenn Sie bei der ersten Einrichtung Ihrer landing zone IAM Identity Center als Identitätsanbieter ausgewählt haben oder wenn Sie anschließend Ihre landing zone Zone-Einstellungen ändern, um IAM Identity Center für Ihre landing zone zu aktivieren. Wenn Sie einen anderen Identitätsanbieter verwenden, haben Sie keinen Zugriff, um diese Baseline zu aktivieren.

- Name (Name: `BackupCentralVaultBaseline`

  Beschreibung: Richtet den zentralen AWS Backup Tresor in Ihrer Organisation ein.
- Name (Name: `BackupAdminBaseline`

  Beschreibung: Richtet den delegierten Administrator und den AWS Backup Audit Manager ein.

Teilweise Registrierung von Konten

Wenn Sie mit Baselines arbeiten, kann ein Konto in den Status Teilweise registriert versetzt werden.

Dieser Status kann auftreten, wenn Sie eine Organisationseinheit erneut registrieren, indem Sie die `ResetEnabledBaseline` API aufrufen, da AWS Control Tower nur die obligatorischen Ressourcen auf die Konten in der Ziel-OU anwendet. Ein Konto, dem die optionalen Ressourcen (Kontrollen) für die übergeordnete Organisationseinheit fehlen, wird als Teilweise registriert markiert.

Wenn Sie ein nicht registriertes Konto in eine registrierte OU verschieben und dann die `ResetEnabledBaseline` API auf der OU aufrufen, um dieses Konto zu registrieren, wendet AWS Control Tower die damit verknüpften Ressourcen auf das neu registrierte Konto `AWSControlTowerBaseline` an. Optionale Kontrollen, die für diese Organisationseinheit aktiviert sind, werden jedoch nicht auf das Konto angewendet. Das Konto befindet sich weiterhin im Status Teilweise registriert.

Um das Konto vollständig zu registrieren, wählen Sie in der Konsole Re-registeroder Konto aktualisieren. Wenn Sie diese Operationen in der Konsole auswählen, wendet AWS Control Tower alle Ressourcen dieser Organisationseinheit auf das neu registrierte Konto an, einschließlich der optionalen Kontrollen, die für diese Organisationseinheit aktiviert sind.

Unterschiede im Betrieb zwischen der AWS Control Tower Tower-Konsole und APIs für Baselines

Wenn Sie den Governance-Status einer Organisationseinheit ändern, führt die AWS Control Tower Tower-Konsole automatisch mehr Operationen für Sie aus, als wenn Sie die Governance mithilfe der APIs für Baselines ändern würden.

Unterschiede

- Registrierung und Bereitstellung von Produkten

Wenn Sie eine Organisationseinheit über die Konsole registrieren, erstellt AWS Control Tower im Rahmen der Registrierung der einzelnen Konten Service Catalog-Produkte für die Mitgliedskonten der Organisationseinheit. Wenn Sie eine Organisationseinheit über die `EnableBaseline` API und die registrieren`AWSControlTowerBaseline`, erstellt AWS Control Tower keine bereitgestellten Produkte für die Mitgliedskonten in der Organisationseinheit.

- Eine Organisationseinheit abmelden

  Jedes Mal, wenn Sie eine Organisationseinheit abmelden, müssen Sie zunächst alle Mitgliedskonten und verschachtelten Organisationseinheiten entfernen. Anschließend entfernt AWS Control Tower alle Kontrollen, die auf die Organisationseinheit angewendet wurden.

  - Wenn Sie in der Konsole die OU löschen auswählen, fährt AWS Control Tower mit der Abmeldung fort und löscht dann die OU aus Ihrer Organisation.
  - Wenn Sie die OU jedoch abmelden, indem Sie die `DisableBaseline` API aufrufen, um sie `AWSControlTowerBaseline` aus der OU zu entfernen, löscht AWS Control Tower die OU nicht aus Ihrer Organisation, die OU ist immer noch in der Organisation vorhanden, nicht registriert.

Aktivierte Baselines und Mitgliedskonten

Wenn Sie eine Basiskonfiguration für eine Organisationseinheit aktivieren, wird diese Konfiguration von den Mitgliedskonten der Organisationseinheit übernommen. Aufgrund der Tatsache der Vererbung sprechen wir von einer Baseline mit aktiviertem Kind, wenn wir uns auf das Konto beziehen. Die Baseline, die auf die Organisationseinheit angewendet wird, wird als Baseline mit aktiviertem Elternteil bezeichnet. Die übergeordnete aktivierte Baseline steuert die Konfiguration ihrer untergeordneten aktivierten Baselines. Es ähnelt der Art und Weise, wie ein Steuerelement, wenn es in einer Organisationseinheit aktiviert ist, für jedes Konto innerhalb der Organisationseinheit gilt.

Den Basisstatus eines Kontos anzeigen

Mit AWS Control Tower können Sie Konten nicht direkt mit Baselines ansprechen. Sie können jedoch den Aktivierungs- und Drift-Status jedes Mitgliedskontos anhand der Baselines nachverfolgen, die für das jeweilige Mitgliedskonto aktiviert wurden. Um den Status Ihrer Konten einzusehen, können Sie die `ListEnabledBaselines`API mit dem Feature-Flag aufrufen. `includeChildren`

Deaktivieren Sie die Baseline eines Kontos

AWS Control Tower erlaubt es Ihnen nicht, eine untergeordnete aktivierte Baseline zu deaktivieren, die mit einer übergeordneten aktivierten Baseline verknüpft ist. Eine Baseline, für die ein Kind aktiviert ist, kann deaktiviert werden, wenn sie vererbt und nicht mehr mit einer Baseline verknüpft ist, für die ein Elternteil aktiviert ist.

Baselines und Standardeinstellungen für die Versionierung

Wenn Ihre AWS Control Tower-Landezone bereits eingerichtet ist und Sie sich dann dafür entscheiden, eine Landingzone-Baseline zu aktivieren, aktiviert AWS Control Tower die neueste Version der Baseline, die mit Ihrer Landingzone-Version kompatibel ist. Wenn Sie sich dafür entscheiden, eine Baseline für eine OU zu aktivieren, die noch nicht bei AWS Control Tower registriert ist, stellt AWS Control Tower automatisch die neueste kompatible Version der Baseline für diese OU bereit.

Kompatibilität von OU-Baselines und landing zone Zone-Versionen

Mit AWS Control Tower Tower-Baselines können Sie einen Governance-Standard auf OU-Ebene und nicht auf Landingzone-Ebene festlegen, falls Ihr Unternehmen dies erfordert. Die aufgerufene Baseline `AWSControlTowerBaseline` ist verfügbar, um Ihnen bei der Registrierung Ihrer Organisationseinheiten bei AWS Control Tower zu helfen.

> **Note**
>
> Eine Baseline ist eine Gruppe von Kontrollen und Ressourcen, die zusammenarbeiten, um ein stabiles Governance-Umfeld in Ihrer landing zone zu schaffen.

Wenn Sie eine Baseline auf einer Organisationseinheit aktivieren, indem Sie die `EnableBaseline` API in AWS Control Tower aufrufen, müssen Sie eine Basisversion angeben, die mit Ihrer aktuellen AWS Control Tower Tower-Landingzone-Version kompatibel ist. Nachdem Sie eine Baseline angegeben haben, folgen alle Mitgliedskonten in einer OU der für die OU angegebenen Baseline. Mit anderen Worten, neue Konten werden mit der aktualisierten Baseline bereitgestellt, und bestehende Mitgliedskonten werden entsprechend der neuen Baseline verwaltet.

Wenn Sie keine Baseline für Ihre vorhandenen Organisationseinheiten und Konten auswählen, bestimmt die Landingzone-Version standardmäßig den gesamten Governance-Status. Jeder registrierten Organisationseinheit in Ihrer landing zone wird jedoch eine Baseline-Version

zugewiesen. Dabei handelt es sich um die neueste Baseline-Version, die mit Ihrer aktuellen Landingzone-Version kompatibel ist. Daher ist jeder Organisationseinheit und jedem registrierten Mitgliedskonto eine Basisversion zugeordnet, auch wenn Sie nie speziell eine Basisversion zuweisen.

Für die OU-level Baseline zeigt die folgende Tabelle die Kompatibilität der Baselines mit den Versionen der AWS Control Tower landing zone. `AWSControlTowerBaseline`

Basisversion	Versionen für Landezonen	Enthaltene Baupläne	Änderung gegenüber dem vorherigen Basisplan		
1,0	2,0 auf 2,7	BP_BASELINE_CLOUDTRAIL, BP_BASELINE_CLOUDWATCH, BP_BASELINE_CONFIG, BP_BASELINE_ROLES, BP_BASELINE_SERVICE_ROLES, IAM-Ressourcen	Keine		
2.0	2.8 bis 2.9	BP_BASELINE_CLOUDTRAIL, BP_BASELINE_CLOUDWATCH, BP_BASELINE_CONFIG	AWS Config Service-Linked Role (SLR) und neuer Config-Blueprint zur Verwendun		

Basisversion	Versionen für Landezonen	Enthaltene Baupläne	Änderung gegenüber dem vorherigen Basisplan		
		, BP_BASELINE_ROLES, BP_BASELINE_SERVICE_ROLES, Config SLR, IAM-Ressourcen	g der SLR hinzugefügt		
3.0	3.0 bis 3.1	BP_BASELINE_CLOUDWATCH, BP_BASELINE_CONFIG, BP_BASELINE_ROLES, BP_BASELINE_SERVICE_ROLES, Config SLR, IAM-Ressourcen	Neuer AWS Config Entwurf. Ändern Sie, um globale Ressourcen nur in der Heimatregion aufzuzeichnen. Der CloudTrail Blueprint wurde entfernt		

Basisversion	Versionen für Landezonen	Enthaltene Baupläne	Änderung gegenüber dem vorherigen Basisplan		
4,0	3.2 bis 3.3	BP_BASELINE_CLOUDWATCH, BP_BASELINE_CONFIG, BP_BASELINE_ROLES, BP_BASELINE_SERVICE_LINKED_ROLE, BP_BASELINE_SERVICE_ROLES, Config SLR, IAM-Ressourcen	Neuer SLR-Blueprint		

Basisversion	Versionen für Landezonen	Enthaltene Baupläne	Änderung gegenüber dem vorherigen Basisplan		
5.0	4,0	BP_BASELINE_CLOUDWATCH, BP_BASELINE_CONFIG, BP_BASELINE_ROLES, BP_BASELINE_SERVICE_LINKED_ROLE, BP_BASELINE_SERVICE_ROLES, Config SLR, IAM-Ressourcen	Die AWS Config Aggregation-Autorisierung(en) wurden entfernt. AWS Config Aggregation Eine Autorisierung für jedes Mitgliedskonto ist nicht erforderlich, da in LandingZone Version 4.0 der AWS Organizations Config Aggregator eingeführt wurde, der Zugriff auf alle Mitgliedskonten innerhalb der Organisation hat.		

Weitere Informationen zu bestimmten Ressourcen, die bei der Einrichtung Ihrer landing zone in Konten erstellt wurden, finden Sie unter In geteilten Konten erstellte Ressourcen.

Wenn Sie Ihre landing zone auf eine Version aktualisieren, die eine neuere `AWSControlTowerBaseline` Basisversion unterstützt, und die neue landing zone Zone-Version mit Ihrer vorhandenen Basisversion kompatibel ist, ändert sich Ihr OU-Status in Update verfügbar.

- Sie können Account Factory und andere Funktionen weiterhin verwenden, ohne die Basislinie der Organisationseinheit (OU) sofort zu aktualisieren.
- Neue Konten, die in dieser Organisationseinheit registriert sind, erhalten Ressourcen auf der Grundlage der vorhandenen Basisversion, bis die Basisversion aktualisiert wird (mit der Funktion „Verwaltung erweitern“ in der Konsole oder mithilfe der `UpdateEnabledBaseline` API).
- Nachdem Sie die Basisversion aktualisiert haben, erhalten alle Konten in dieser Organisationseinheit Ressourcen, die auf der neuen Basisversion basieren.

> **Note**
>
> Wenn Ihre Organisationseinheiten nach dem Update Ihrer AWS Control Tower Tower-Landingzone-Version in der Konsole den Status Update erforderlich anzeigen, müssen Sie die Basisversion dieser Organisationseinheiten aktualisieren.

Überlegungen zu Baselines

- Wenn für Ihre Organisationseinheit ein Basisupdate erforderlich ist, können Sie keine neuen Konten bereitstellen oder bestehende Konten für diese Organisationseinheit registrieren.
- Wenn Sie nach einem landing zone Zone-Update auch eine OU-Baseline aktualisieren möchten, müssen Sie die OU erneut registrieren oder Ihre OU-Baseline-Version programmgesteuert aktualisieren.
- Wir empfehlen Ihnen, auf die höchste kompatible Baseline für die von Ihnen verwendete landing zone Zone-Version zu aktualisieren, damit Sie alle Vorteile der landing zone und der Baseline zusammen nutzen können. Wenn Sie beispielsweise auf landing zone Version 3.3 aktualisieren, können Sie Baseline 3.0 weiterhin verwenden, aber Sie können nicht alle Vorteile von landing zone Version 3.3 nutzen, es sei denn, Sie aktualisieren auch auf Baseline 4.0.
- Baseline-Updates können nicht rückgängig gemacht werden.

- Die Basisaktivierung zielt jeweils auf eine Organisationseinheit ab. Daher werden verschachtelte Organisationseinheiten nicht automatisch aktualisiert, wenn die übergeordnete Organisationseinheit aktualisiert wird. Es wird empfohlen, die übergeordnete Organisationseinheit zu aktualisieren, bevor Sie die verschachtelten Organisationseinheiten aktualisieren.
- Wenn Sie die `UpdateEnabledBaseline` API aufrufen oder eine Organisationseinheit von der Konsole aus erneut registrieren, behält die Organisationseinheit alle Steuerelemente bei, die vor dem Baseline-Update aktiviert wurden.
- Wenn mehrere Basisversionen mit Ihrer landing zone Zone-Version kompatibel sind, müssen Sie die neueste Basisversion verwenden, wenn Sie eine Baseline-Version auf einer nicht verwalteten Organisationseinheit aktivieren.

Beispiele: Registrieren Sie eine AWS Control Tower-OU nur mit APIs

Diese exemplarische Vorgehensweise mit Beispielen ist ein Begleitdokument. Erläuterungen, Vorbehalte und weitere Informationen finden Sie unter. Arten von Basislinien

Voraussetzungen

Sie müssen über eine bestehende OU verfügen, die nicht bei AWS Control Tower registriert ist und die Sie registrieren möchten. Oder Sie müssen über eine registrierte OU verfügen, die Sie zur Aktualisierung erneut registrieren möchten.

Registrieren Sie eine OU

1. Prüfen Sie, ob `IdentityCenterBaseline` das für die Landezone aktiviert ist. Wenn ja, rufen Sie den Identity Center Enabled Baseline-Identifier ab.

```
aws controltower list-baselines --query 'baselines[?name==`IdentityCenterBaseline`].
[arn]'
```

```
aws controltower list-enabled-baselines --query 'enabledBaselines[?
baselineIdentifier==`<Identity Center Baseline Arn>`].[arn]'
```

2. Ruft den ARN der Ziel-OU ab.

```
aws organizations describe-organizational-unit --organizational-unit-id
 <Organizational Unit ID> --query 'OrganizationalUnit.[Arn]'
```

3. Ruft den ARN der `AWSControlTowerBaseline` Basislinie ab.

```
aws controltower list-baselines --query 'baselines[?name==`AWSControlTowerBaseline`].
[arn]'
```

4. Erstellen Sie die `AWSControlTowerBaseline` Baseline auf der Ziel-OU.

   Wenn die Identity Center Baseline aktiviert ist:

```
aws controltower enable-baseline --baseline-identifier <AWSControlTowerBaseline ARN>
 --baseline-version <BASELINE VERSION> --target-identifier <OU ARN> --parameters
 '[{"key":"IdentityCenterEnabledBaselineArn","value":"<Identity Center Enabled
 Baseline ARN>"}]'
```

   Wenn die Identity Center Baseline nicht aktiviert ist, lassen Sie das *`parameters`* Flag wie folgt weg:

```
aws controltower enable-baseline --baseline-identifier <AWSControlTowerBaseline ARN>
 --baseline-version <BASELINE VERSION> --target-identifier <OU ARN>
```

Re-register Eine OU

Nachdem Sie die Einstellungen der Landezone aktualisiert oder Ihre Landing Zone-Version aktualisiert haben, müssen Sie Re-register die OUs auf die neuesten Änderungen übertragen. Gehen Sie wie folgt vor, um eine Organisationseinheit programmgesteuert erneut zu registrieren, indem Sie die zugehörige `EnabledBaseline` Ressource und alle zugehörigen Ressourcen zurücksetzen. `EnabledControl`

> **Important**
>
> Wenn für die Organisationseinheit optionale Steuerelemente aktiviert sind, müssen Sie nach dem Zurücksetzen der Baseline auch die `ResetEnabledControl` API für jedes aktivierte optionale Steuerelement aufrufen. Dieser Schritt stellt sicher, dass die optionalen Steuerungen mit der neuesten Landezonenkonfiguration konsistent bleiben. Wenn Sie diesen

Schritt überspringen, spiegeln die optionalen Steuerelemente in der Organisationseinheit möglicherweise nicht die neuesten Änderungen der Landezone wider. Wenn Sie keine optionalen Steuerelemente aktiviert haben, ist dieser Schritt nicht erforderlich.

1. Rufen Sie den ARN der Ziel-OU ab, um sich erneut zu registrieren.

```
aws organizations describe-organizational-unit --organizational-unit-id <OU ID> --
query 'OrganizationalUnit.[Arn]'
```

2. Ruft den ARN der `EnabledBaseline` Ressource für die Ziel-OU ab.

```
aws controltower list-enabled-baselines --query 'enabledBaselines[?
targetIdentifier==`<OUARN>`].[arn]'
```

3. Setzen Sie die aktivierte Baseline zurück.

```
aws controltower reset-enabled-baseline --enabled-baseline-
identifier <EnabledBaselineArn>
```

4. Wenn für die OU optionale Steuerelemente aktiviert sind, listen Sie die aktivierten Steuerelemente für die OU auf und setzen Sie sie jeweils zurück, sodass sie mit der aktuellen Landezone-Konfiguration konsistent bleiben.

   Listet die aktivierten Steuerelemente auf der Ziel-OU auf:

```
aws controltower list-enabled-controls --target-identifier <OU ARN>
```

   Setzen Sie jedes zurückgegebene aktivierte optionale Steuerelement zurück, indem Sie Folgendes aufrufen:

```
aws controltower reset-enabled-control --enabled-control-
identifier <EnabledControlArn>
```

   Weitere Informationen finden Sie ResetEnabledControl in der API-Referenz für AWS Control Tower.

Beispiele für die grundlegende API-Nutzung

Dieser Abschnitt enthält Beispiele für Eingabe- und Ausgabeparameter für die AWS Control Tower Tower-Baseline-APIs.

DisableBaseline

Weitere Informationen zu diesem API-Vorgang finden Sie unter DisableBaseline.

`DisableBaseline`Eingabe:

```
{
    "enabledBaselineIdentifier": "arn:aws:controltower:us-
west-2:123456789012:enabledbaseline/AB12CD34EF56GH789"
}
```

`DisableBaseline`Ausgang:

```
{
    "operationIdentifier": "58f12232-26be-4735-a3e9-dd30d90f021f"
}
```

`DisableBaseline`-CLI-Beispiel:

```
aws controltower disable-baseline \
    --enabled-baseline-identifier arn:aws:controltower:us-
west-2:123456789012:enabledbaseline/AB12CD34EF56GH789 \
    --region us-west-2
```

EnableBaseline

Weitere Hinweise zu diesem API-Vorgang finden Sie unter EnableBaseline.

`EnableBaseline`Eingabe:

```
{
    "baselineIdentifier": "arn:aws:controltower:us-west-2::baseline:17BSJV3IGJ2QSGA2",
    "targetIdentifier": "arn:aws:organizations::123456789012:ou/o-kgj0txdhpa/ou-
r9mj-4j3mzjql",
    "baselineVersion": "3.0",
    "parameters": [
```

```
        {
            "key": "IdentityCenterEnabledBaselineArn",
            "value": "arn:aws:controltower:us-west-2:123456789012:enabledbaseline/
XAHCR4CJTSI4W07MZ"
        }
    ]
}
```

`EnableBaseline`Ausgabe, Rückgabe einer neuen Ressource:

```
{
    "operationIdentifier": "58f12232-26be-4735-a3e9-dd30d90f021f",
    "arn": "arn:aws:controltower:us-west-2:123456789012:enabledbaseline/
XAGF7TNOHRD7ES5VV"
}
```

`EnableBaseline`-CLI-Beispiel:

Dieses Beispiel zeigt die Aktivierung einer Baseline für eine AWS Organizations Organisation, deren landing zone den AWS IAM Identity Center-Zugriff aktiviert hat, der von AWS Control Tower verwaltet wird. Um Ihre Identity `EnabledBaseline` Center-ID abzurufen, können Sie die `ListEnabledBaselines` API aufrufen und dabei nach der Identity Center-Baseline filtern: `(arn:aws:controltower:`*`Region`*`::baseline/LN25R72TTG6IGPTQ)`

```
aws controltower list-enabled-baselines \
    --filter baselineIdentifiers=arn:aws:controltower:us-west-2::baseline/
LN25R72TTG6IGPTQ \
    --region us-west-2
```

In der Antwort wird das `EnabledBaseline` Detail angezeigt, in dem auch die Kennung angegeben ist.

```
{
    "enabledBaselines": [
        {
            "arn": "arn:aws:controltower:us-west-2:123456789012:enabledbaseline/
XAHXS7P6C4I453EZC",
            "baselineIdentifier": "arn:aws:controltower:us-west-2::baseline/
LN25R72TTG6IGPTQ",
            "targetIdentifier": "arn:aws:organizations::123456789012:account/o-
aq21sw43de5/123456789012",
```

```
            "statusSummary": {
                "status": "SUCCEEDED"
            }
        }
    ]
}
```

> **Note**
>
> Notieren Sie sich den ARN-Wert aus der Antwort und übergeben Sie diesen Wert als Parameter, um die Standard-Baseline zu aktivieren.

```
aws controltower enable-baseline \
    --baseline-identifier arn:aws:controltower:us-west-2::baseline/17BSJV3IGJ2QSGA2 \
    --baseline-version 3.0 \
    --target-identifier arn:aws:organizations::123456789012:ou/o-aq21sw43de5/ou-po90-
lk87jh65 \
    --parameters
 '[{"key":"IdentityCenterEnabledBaselineArn","value":"arn:aws:controltower:us-
west-2:123456789012:enabledbaseline/XAHXS7P6C4I453EZC"}]' \
    --region us-west-2
```

Für eine Organisation, deren landing zone vom AWS Control Tower Tower-Management von IAM Identity Center abgemeldet ist, aktivieren Sie die Baseline ohne den Parameter.

```
aws controltower enable-baseline \
    --baseline-identifier arn:aws:controltower:us-west-2::baseline/17BSJV3IGJ2QSGA2 \
    --baseline-version 3.0 \
    --target-identifier arn:aws:organizations::123456789012:ou/o-aq21sw43de5/ou-po90-
lk87jh65 \
    --region us-west-2
```

`GetBaseline`

Weitere Informationen zu diesem API-Vorgang finden Sie unter. GetBaseline

`GetBaseline`Eingabe:

```
{
```

```
    "baselineIdentifier": "arn:aws:controltower:us-west-2::baseline/17BSJV3IGJ2QSGA2"
}
```

`GetBaseline`Ausgang:

```
{
    "arn": "arn:aws:controltower:us-west-2::baseline/17BSJV3IGJ2QSGA2",
    "name": "AWSControlTowerBaseline",
    "description": "Sets up resources and mandatory controls for member accounts within
 the target OU, required for AWS Control Tower governance.",
}
```

`GetBaseline`-CLI-Beispiel:

```
aws controltower get-baseline \
    --baseline-identifier arn:aws:controltower:us-west-2::baseline/17BSJV3IGJ2QSGA2 \
    --region us-west-2
```

`GetBaselineOperation`

Weitere Hinweise zu diesem API-Vorgang finden Sie unter GetBaselineOperation.

`GetBaselineOperation`Eingabe:

```
{
    "operationIdentifier": "58f12232-26be-4735-a3e9-dd30d90f021f"
}
```

`GetBaselineOperation`Ausgang:

```
{
    "baselineOperation": {
        "operationIdentifier": "58f12232-26be-4735-a3e9-dd30d90f021f",
        "operationType": "DISABLE_BASELINE",
        "status": "FAILED",
        "startTime": "2023-01-12T19:05:00Z",
        "endTime": "2023-01-12T19:45:00Z",
        "statusMessage": "Can't perform DisableBaseline on a parent target with
 governed child OUs"
    }
}
```

GetBaselineOperation-CLI-Beispiel:

```
aws controltower get-baseline-operation \
    --operation-identifier 58f12232-26be-4735-a3e9-dd30d90f021f \
    --region us-west-2
```

GetEnabledBaseline

Weitere Hinweise zu diesem API-Vorgang finden Sie unter GetEnabledBaseline.

GetEnabledBaselineEingabe:

```
{
    "enabledBaselineIdentifier": "arn:aws:controltower:us-
west-2:123456789012:enabledbaseline/XAHCR4CJTSI4W07MZ"
}
```

GetEnabledBaselineAusgang:

```
{
    "enabledBaselineDetails": {
        "arn": "arn:aws:controltower:us-west-2:123456789012:enabledbaseline/
XAHCR4CJTSI4W07MZ",
        "baselineIdentifier": "arn:aws:controltower:us-
west-2::baseline:17BSJV3IGJ2QSGA2",
        "baselineVersion": "3.0",
        "targetIdentifier": "arn:aws:organizations::123456789012:ou/o-kgj0txdhpa/ou-
r9mj-4j3mzjql",
        "statusSummary": {
            "status": "SUCCEEDED",
            "lastOperationIdentifier": "58f12232-26be-4735-a3e9-dd30d90f021f"
        },
        "parameters": [
            {
                "key": "IdentityCenterEnabledBaselineArn",
                "value": "arn:aws:controltower:us-west-2:123456789012:enabledbaseline/
XAHCR4CJTSI4W07MZ"
            }
        ]
    }
}
```

`GetEnabledBaseline`-CLI-Beispiel:

```
aws controltower get-enabled-baseline \
    --enabled-baseline-identifier arn:aws:controltower:us-
west-2:123456789012:enabledbaseline/XAHXS7P6C4I453EZC \
    --region us-west-2
```

`ListBaselines`

Weitere Hinweise zu diesem API-Vorgang finden Sie unter ListBaselines.

`ListBaselines`Eingabe (mit optionalen Eingaben):

```
{
    "nextToken": "AbCd1234",
    "maxResults": "4"
}
```

`ListBaselines`Ausgang:

```
{
    "baselines": [
        {
            "arn": "arn:aws:controltower:us-east-1::baseline/4T4HA1KMO10S6311",
            "name": "AuditBaseline",
            "description": "Sets up resources to monitor security and compliance of
 accounts in your organization."
        },
        {
            "arn": "arn:aws:controltower:us-east-1::baseline/J8HX46AHS5MIKQPD",
            "name": "LogArchiveBaseline",
            "description": "Sets up a central repository for logs of API activities and
 resource configurations from accounts in your organization."
        },
        {
            "arn": "arn:aws:controltower:us-east-1::baseline/LN25R72TTG6IGPTQ",
            "name": "IdentityCenterBaseline",
            "description": "Sets up shared resources for AWS Identity Center, which
 prepares the AWSControlTowerBaseline to set up Identity Center access for accounts."
        },
        {
            "arn": "arn:aws:controltower:us-east-1::baseline/17BSJV3IGJ2QSGA2",
```

```
            "name": "AWSControlTowerBaseline",
            "description": "Sets up resources and mandatory controls for member
 accounts within the target OU, required for AWS Control Tower governance."
        },
        {
            "arn": "arn:aws:controltower:us-east-1::baseline/3WPD0NA6TJ9AOMU2",
            "name": "BackupCentralVaultBaseline",
            "description": "Sets up central AWS Backup vault in your organization."
        },
        {
            "arn": "arn:aws:controltower:us-east-1::baseline/H6C5JFCJJ3CPU3J5",
            "name": "BackupAdminBaseline",
            "description": "Sets up delegated admin and AWS Backup Audit Manager."
        },
        {
            "arn": "arn:aws:controltower:us-east-1::baseline/APO9ATVPBKFRRGLK",
            "name": "BackupBaseline",
            "description": "Sets up local Backup vault and attach Backup policy."
        }
    ]
}
```

`ListBaselines`-CLI-Beispiel:

```
aws controltower list-baselines \
    --region us-west-2
```

`ListEnabledBaselines`

Die `ListEnabledBaselines` API verfügt über einen optionalen Parameter, mit dem Sie sich die Baselines anzeigen lassen können, die für die Konten gelten, die Mitglieder einer Organisationseinheit sind. Die folgenden Beispiele zeigen einige CLI-Befehle, mit denen Sie die Baselines für ein Konto anzeigen können. AWS Control Tower bezeichnet diese Baselines, die in der OU aktiviert sind, aber für jedes Konto innerhalb der OU gelten, als untergeordnete aktivierte Baselines, da sie ihre Governance-Konfiguration von den Baselines ableiten, die auf der OU angewendet werden.

Weitere Informationen zu diesem API-Vorgang finden Sie unter. ListEnabledBaselines

`ListEnabledBaselines`Eingabe zum Anzeigen von Baselines, für die das untergeordnete Element aktiviert ist:

```
aws controltower list-enabled-baselines --include-children
```

`ListEnabledBaselines`Ausgabe zum Anzeigen von Baselines, für die das untergeordnete Element aktiviert ist:

```
{
    "enabledBaselines": [
        {
            "arn": "arn:aws:controltower:us-east-1:666355521292:enabledbaseline/
XO2UQ1PC6BB5085S5",
            "baselineIdentifier": "arn:aws:controltower:us-east-1::baseline/
APO9ATVPBKFRRGLK",
            "baselineVersion": "1.0",
            "statusSummary": {
                "lastOperationIdentifier": "07d6d2b8-e357-4f96-ba00-98ea88143445",
                "status": "SUCCEEDED"
            },
            "targetIdentifier": "arn:aws:organizations::666355521292:ou/o-vaex10vaey/
ou-k86y-ld9k8vpu"
        },
        {
            "arn": "arn:aws:controltower:us-east-1:666355521292:enabledbaseline/
XAFPKQQXOJB50ZWQH",
            "baselineIdentifier": "arn:aws:controltower:us-east-1::baseline/
APO9ATVPBKFRRGLK",
            "baselineVersion": "1.0",
            "parentIdentifier": "arn:aws:controltower:us-
east-1:666355521292:enabledbaseline/XOIZ4G08CWB50ZWON",
            "statusSummary": {
                "lastOperationIdentifier": "3508793e-48c8-4895-965b-3dc6abd52b6b",
                "status": "SUCCEEDED"
            },
            "targetIdentifier": "arn:aws:organizations::666355521292:account/o-
vaex10vaey/183295447314"
        }
]
```

> **Note**
>
> Im vorherigen Beispiel zeigt das `parentIdentifier` Feld die aktivierte Baseline der übergeordneten Organisationseinheit für diese untergeordnete Basislinie an.

Alle Baselines anzeigen, die auf ein bestimmtes Ziel (OU oder Konto) angewendet wurden:

```
aws controltower list-enabled-baselines \
    --filter '{
        "targetIdentifiers": ["TARGET_ARN"]
    }
```

Alle Organisationseinheiten anzeigen, die eine bestimmte Baseline haben:

```
aws controltower list-enabled-baselines \
    --filter '{
        "baselineIdentifiers": ["BASELINE_ARN"]
    }'
```

Alle Organisationseinheiten und Konten mit einem bestimmten Basiswert anzeigen:

```
aws controltower list-enabled-baselines \
    --filter '{
        "baselineIdentifiers": ["BASELINE_ARN"]
    }'  \
    --include-children
```

Alle Konten in einer Organisationseinheit anzeigen, für die Baseline B aktiviert ist:

```
### First fetch the enabled baseline record for Baseline B on the OU
 aws controltower list-enabled-baselines \
    --filter '{
        "targetIdentifiers": ["OU_TARGET_ARN"],
        "baselineIdentifiers": ["BASELINE_ARN_FOR_BASELINE_B"]
    }'

### Call ListEnabled baseline to fetch all accounts that have their parent as the
 enabled baseline record on the OU
aws controltower list-enabled-baselines \
    --filter '{
        "parentIdentifiers": ["ENABLED_BASELINE_ARN_FOR_OU"]
    }' \
    --include-children
```

Weitere Informationen zu Baselines, für die Kinder aktiviert sind

- Sie können die `GetEnabledBaseline` API verwenden, um detaillierte Informationen zu einer bestimmten Baseline mit aktiviertem Kind abzurufen
- Sie können die `GetBaselineOperation` API verwenden, um einen Vorgang anzuzeigen, der auf der Baseline mit aktiviertem Kind ausgeführt wurde
- Sie können keine Schreib-APIs, wie,, `ResetEnabledBaseline` oder, für eine Baseline `EnableBaselineUpdateEnabledBaseline`, für die ein untergeordnetes Element aktiviert ist`DisableBaseline`, direkt aufrufen.
- Untergeordnete Basisressourcen können nur mithilfe des AWS Control Tower Tower-Service, durch Operationen, die auf der übergeordneten Organisationseinheit ausgeführt werden, oder mithilfe von Account Factory geändert werden.

Beispiele für die Verwendung von Filtern:

`ListEnabledBaselines`Eingabe (keine Filter):

```
{
    "nextToken": "bde7-XX0c6fXXXXXX",
    "maxResults": 5
}
```

`ListEnabledBaselines`Eingabe (nur `baselineIdentifiers` Filter):

```
{
    "filter": {
        "baselineIdentifiers": ['arn:aws:controltower:us-
east-1::baseline/17BSJV3IGJ2QSGA2', 'arn:aws:controltower:us-
east-1::baseline/12GZU8CKZKVMS2AW']
    },
    "nextToken": "bde7-XX0c6fXXXXXX",
    "maxResults": 5
}
```

`ListEnabledBaselines`Eingabe (nur `targetIdentifiers` Filter):

```
{
    "filter": {
```

```
        "targetIdentifiers": ['arn:aws:organizations::123456789012:ou/o-s9511vn103/ou-
xqj7-fex1u317', 'arn:aws:organizations::123456789012:ou/o-s9511vn103/ou-xqj7-11q6n2cf']
    },
    "nextToken": "bde7-XX0c6fXXXXXX",
    "maxResults": 2
}
```

`ListEnabledBaselines`Eingabe (`baselineIdentifiers`sund `targetIdentifiers` Filter):

```
{
    "filter": {
        "baselineIdentifiers": ['arn:aws:controltower:us-
east-1::baseline/17BSJV3IGJ2QSGA2']
        "targetIdentifiers": ['arn:aws:organizations::123456789012:ou/o-s9511vn103/ou-
xqj7-fex1u317']
    },
    "nextToken": "bde7-XX0c6fXXXXXX",
    "maxResults": 5
}
```

`ListEnabledBaselines`Ausgang:

```
{
    "enabledBaselines": [
        {
            "arn": "arn:aws:controltower:us-east-1:123456789012:enabledbaseline/
XAHCR4CJTSI4W07MZ",
            "baselineIdentifier": "arn:aws:controltower:us-
east-1::baseline:17BSJV3IGJ2QSGA2",
            "baselineVersion": "3.0",
            "targetIdentifier": "arn:aws:organizations::123456789012:ou/o-kgj0txdhpa/
ou-r9mj-4j3mzjql",
            "statusSummary": {
                "status": "SUCCEEDED",
                "lastOperationIdentifier": "58f12232-26be-4735-a3e9-dd30d90f021f"
            }
        },
        {
            "arn": "arn:aws:controltower:us-east-1:123456789012:enabledbaseline/
XAJ9NKW88AA4W9CLL",
            "baselineIdentifier": "arn:aws:controltower:us-
east-1::baseline:17BSJV3IGJ2QSGA2",
            "baselineVersion": "4.0",
```

```
            "targetIdentifier": "arn:aws:organizations::123456789012:ou/o-s9511vn103/
ou-xqj7-fex1u317",
            "statusSummary": {
            "status": "FAILED",
                "lastOperationIdentifier": "81e02df1-2b4d-48f0-838f-3833b93dcdc0"
            }
        }
    ],
    "nextToken": "e2bXXXXX6cab"
}
```

CLI-Beispiel mit einem Filtertyp (`baselineIdentifiers`Filter):

```
aws controltower list-enabled-baselines \
    --filter baselineIdentifiers=arn:aws:controltower:us-
west-2::baseline/17BSJV3IGJ2QSGA2,arn:aws:controltower:us-west-2::baseline/
LN25R72TTG6IGPTQ \
    --region us-west-2
```

CLI-Beispiel mit mehreren Filtern (`baselineIdentifiers`und `targetIdentifiers` Filtern):

```
aws controltower list-enabled-baselines \
    --filter targetIdentifiers=arn:aws:organizations::123456789012:ou/o-
aq21sw43de5/ou-po90-lk87jh65,baselineIdentifiers=arn:aws:controltower:us-
west-2::baseline/17BSJV3IGJ2QSGA2 \
    --region us-west-2
```

`ResetEnabledBaseline`

Weitere Informationen zu diesem API-Vorgang finden Sie unter ResetEnabledBaseline.

`ResetEnabledbaseline`Eingabe:

```
{
    "enabledBaselineIdentifier": "arn:aws:controltower:us-
west-2:123456789012:enabledbaseline/XAJ9NKW88AA4W9CLL"
}
```

`ResetEnabledBaseline`Ausgang:

```
{
```

```
    "operationIdentifier": "81e02df1-2b4d-48f0-838f-3833b93dcdc0"
}
```

`ResetEnabledBaseline`-CLI-Beispiel:

```
aws controltower reset-enabled-baseline \
    --enabled-baseline-identifier arn:aws:controltower:us-
west-2:123456789012:enabledbaseline/XAHXS7P6C4I453EZC \
    --region us-west-2
```

`UpdateEnabledBaseline`

Weitere Hinweise zu diesem API-Vorgang finden Sie unter UpdateEnabledBaseline.

`UpdateEnabledBaseline`Eingabe:

```
{
    "enabledBaselineIdentifier": "arn:aws:controltower:us-
east-1:123456789012:enabledbaseline/XAJ9NKW88AA4W9CLL",
    "baselineVersion": "4.0",
    "parameters": [
        {
            "key": "IdentityCenterEnabledBaselineArn",
            "value": "arn:aws:controltower:us-east-1:123456789012:enabledbaseline/
XAHCR4CJTSI4W07MZ"
        }
    ]
}
```

`UpdateEnabledBaseline`Ausgang:

```
{
    "operationIdentifier": "81e02df1-2b4d-48f0-838f-3833b93dcdc0"
}
```

`UpdateEnabledBaseline`-CLI-Beispiel:

```
aws controltower update-enabled-baseline \
    --enabled-baseline-identifier arn:aws:controltower:us-
west-2:123456789012:enabledbaseline/XAHXS7P6C4I453EZC \
    --baseline-version 4.0
```

```
    --parameters
 '[{"key":"IdentityCenterEnabledBaselineArn","value":"arn:aws:controltower:us-
west-2:123456789012:enabledbaseline/XAHXS7P6C4I453EZC"}]' \
    --region us-west-2
```

Zusätzliche Informationen und Links

Dieses Thema enthält Links zu relevanten Blogbeiträgen, technischer Dokumentation und verwandten Informationen, die Ihnen bei der Arbeit mit AWS Control Tower helfen können. Die Quellen behandeln einige gängige Anwendungsfälle und bewährte Methoden für die Funktionen von AWS Control Tower sowie einige zusätzliche Verbesserungen.

Tutorials und Übungen

- AWS Control Tower-Labor — Diese Labs bieten einen allgemeinen Überblick über allgemeine Aufgaben im Zusammenhang mit AWS Control Tower.
- Wählen Sie im AWS Control Tower-Dashboard die Option Personalisierte Anleitung abrufen aus, wenn Sie einen Anwendungsfall im Kopf haben, sich aber nicht sicher sind, wo Sie anfangen sollen.
- Besuchen Sie diese AWS Cloud YouTube Operations-Playlist und durchsuchen Sie den AWS Control Tower, um Videos zu finden, in denen mehr über die Nutzung der Funktionen von AWS Control Tower erklärt wird.

Netzwerk

Richten Sie wiederholbare und verwaltbare Muster für Netzwerke in ein. AWS Erfahren Sie mehr über Design, Automatisierung und Appliances, die häufig von Kunden verwendet werden.

- AWS VPC-Architektur für den Schnellstart — Diese Kurzanleitung bietet eine Netzwerkgrundlage, die auf AWS Best Practices für Ihre AWS Cloud-Infrastruktur basiert. Es erstellt eine AWS Virtual Private Network Umgebung mit öffentlichen und privaten Subnetzen, in der Sie AWS Dienste und andere Ressourcen starten können.
- Self-service VPCs im AWS Control Tower mithilfe von AWS Service Catalog — In diesem Blogbeitrag wird beschrieben, wie Sie Account Factory einrichten können, sodass Sie Konten mit benutzerdefinierten VPCs bereitstellen können.
- Implementierung von Serverless Transit Network Orchestrator (STNO) im AWS Control Tower — Dieser Blogbeitrag zeigt, wie der kontoübergreifende Zugriff auf Netzwerkkonnektivität automatisiert werden kann. Dieser Blog richtet sich an AWS Control Tower-Administratoren oder an Personen, die für die Verwaltung von Netzwerken in ihrer Umgebung verantwortlich sind. AWS

Sicherheit, Identität und Protokollierung

Erweitern Sie Ihr Sicherheitsniveau, integrieren Sie externe oder bestehende Identitätsanbieter und zentralisieren Sie die Protokollierungssysteme.

Sicherheit

- Automatisieren von AWS Security Hub CSPM Warnmeldungen bei Ereignissen im AWS Control Tower-Lebenszyklus — In diesem Blogbeitrag wird beschrieben, wie die Aktivierung und Konfiguration von Security Hub CSPM in einer AWS Control Tower-Umgebung mit mehreren Konten für bestehende und neue Konten automatisiert werden kann.
- Aktivierung AWS Identity and Access Management — In diesem Blogbeitrag wird beschrieben, wie Sie die Sichtbarkeit Ihrer Unternehmenssicherheit verbessern können, indem Sie die Ergebnisse von IAM Access Analyzer aktivieren und zentralisieren.
- AWS Systems Manager Parameter Store bietet sicheren, hierarchischen Speicher für die Verwaltung von Konfigurationsdaten und Geheimnissen. Sie können ihn verwenden, um Konfigurationsinformationen an einem sicheren Ort zur Verwendung durch AWS Systems Manager und AWS CloudFormation auszutauschen. Sie können beispielsweise eine Liste der Regionen speichern, in denen Sie Konformitätspakete bereitstellen möchten.

Identität

- Verknüpfen Sie die Azure AD-Benutzeridentität mit AWS Konten und Anwendungen für Single Sign-On — In diesem Blogbeitrag wird beschrieben, wie Sie Azure AD mit IAM Identity Center und AWS Control Tower verwenden.
- Zentrales Verwalten des Zugriffs auf AWS für Okta-Benutzer mit AWS IAM Identity Center — In diesem Blogbeitrag wird beschrieben, wie Okta mit IAM Identity Center und AWS Control Tower verwendet wird.

Protokollierung

- AWS Zentralisierte Protokollierungslösung — In diesem Lösungsbeitrag wird die Centralized Logging-Lösung beschrieben, mit der Unternehmen Protokolle für mehrere Konten und Regionen sammeln, analysieren und anzeigen können. AWS AWS
- Informationen zum Anzeigen Ihrer AWS Config Ressourcen finden Sie im Config Resource Compliance Dashboard.

Bereitstellung von Ressourcen und Verwaltung von Workloads

Stellen Sie Ressourcen und Workloads bereit und verwalten Sie sie.

- Erste Schritte mit der Bibliotheksintegration — In diesem Blogbeitrag werden Portfolios für die ersten Schritte beschrieben, die Sie verwenden können.
- Kontinuierliche Bereitstellung von Cloud Custodian im AWS Control Tower

Zusammenarbeit mit bestehenden Organisationen und Konten

Arbeiten Sie mit bestehenden AWS Organisationen und Konten zusammen.

- Konto registrieren — In diesem Benutzerleitfaden wird beschrieben, wie Sie ein vorhandenes AWS Konto bei AWS Control Tower registrieren.
- Ein Konto unter AWS Control Tower einrichten — In diesem Blogbeitrag wird beschrieben, wie Sie AWS Control Tower in Ihren bestehenden AWS Organisationen bereitstellen.
- Erweitern Sie die AWS Control Tower-Governance mithilfe von AWS Config-Konformitätspaketen — In diesem Blogbeitrag wird beschrieben, wie Sie AWS Config Konformitätspakete bereitstellen, um bestehende Konten und Organisationen in die Verwaltung durch AWS Control Tower zu integrieren.
- So erkennen und mildern Sie Guardrail-Verstöße mit AWS Control Tower — In diesem Blogbeitrag wird beschrieben, wie Sie Kontrollen hinzufügen und SNS-Benachrichtigungen abonnieren, sodass Sie per E-Mail über Verstöße gegen die Einhaltung der Kontrollvorschriften informiert werden können.

Automatisierung und Integration

Automatisieren Sie die Kontoerstellung und integrieren Sie Lebenszyklusereignisse mit AWS Control Tower.

- Lebenszyklusereignisse — In diesem Blogbeitrag wird beschrieben, wie Lebenszyklusereignisse mit AWS Control Tower verwendet werden.
- Automatisieren Sie die Kontoerstellung — In diesem Blogbeitrag wird beschrieben, wie Sie die automatische Kontoerstellung in AWS Control Tower einrichten.
- Amazon VPC Flow-Log-Automatisierung — In diesem Blogbeitrag wird beschrieben, wie Amazon VPC Flow Logs in einer Umgebung mit mehreren Konten automatisiert und zentralisiert werden.

- Automatisieren Sie das VPC-Tagging mit AWS Control Tower-Lebenszyklusereignissen — In diesem Blogbeitrag wird beschrieben, wie das Ressourcen-Tagging für VPCs mithilfe von Lebenszyklusereignissen im AWS Control Tower automatisiert werden kann.
- Automatisierte Kontoverwaltung — In diesem Blogbeitrag wird beschrieben, wie Sie Kontoverwaltungsaufgaben nach der Einrichtung Ihrer AWS Control Tower-Umgebung automatisieren können.

Migration von Workloads

Verwenden Sie andere AWS Services mit AWS Control Tower, um die Workload-Migration zu unterstützen.

- CloudEndure Migration — In diesem Blogbeitrag wird beschrieben, wie Sie andere AWS Services mit AWS Control Tower kombinieren CloudEndure können, um die Workload-Migration zu unterstützen.

Zugehörige AWS-Services

AWS Control Tower fungiert als Orchestrierungsebene für AWS Organizations. Daher haben Sie über die Konsole und die APIs von AWS Organizations Zugriff auf über 20 weitere AWS-Services, die mit AWS Control Tower funktionieren. Auf diese zusätzlichen Dienste kann nicht direkt über die AWS Control Tower-Konsole zugegriffen werden.

- Eine vollständige Liste der Dienste, die AWS Control Tower über AWS Organizations zur Verfügung stellt, finden Sie unter AWS-Services, die Sie mit AWS Organizations nutzen können.
- Um die Funktionen für mehrere Konten für diese verwandten AWS-Services zu aktivieren, müssen Sie den vertrauenswürdigen Zugriff aktivieren. Weitere Informationen finden Sie unter Verwenden von AWS-Organisationen mit anderen AWS-Services.

> **Note**
>
> Denken Sie daran, dass AWS IAM Identity Center und AWS Config, für Sie im AWS Control Tower eingerichtet und vollständig integriert AWS CloudTrail sind. Sie müssen Ihre Einstellungen für vertrauenswürdigen Zugriff oder delegierte Administration für diese Dienste nicht ändern.

- Einige AWS Dienste, die über verfügbar sind, AWS Organizations können die delegierte Administration verwenden, darunter AWS Systems Manager und AWS Firewall Manager. Weitere Informationen finden Sie unter Konfiguration eines delegierten Administrators und Aktivieren eines delegierten Administratorkontos für Firewall Manager. Sehen Sie sich auch dieses Video mit dem Titel Sicherheitsgruppen mit AWS Firewall Manager einrichten an.

AWS Marketplace Lösungen

Entdecken Sie Lösungen von AWS Marketplace.

- AWS Control Tower Marketplace — AWS Marketplace bietet eine breite Palette von Lösungen für AWS Control Tower, um Sie bei der Integration von Drittanbietersoftware zu unterstützen. Diese Lösungen helfen bei der Lösung wichtiger infrastruktureller und betrieblicher Anwendungsfälle, darunter Identitätsmanagement, Sicherheit für eine Umgebung mit mehreren Konten, zentralisierte Netzwerke, Betriebsinformationen und Sicherheitsinformations- und Eventmanagement (SIEM).

Versionshinweise zu AWS Control Tower

Die folgenden Abschnitte enthalten Details zu den Versionen von AWS Control Tower seit der Einführung des Service. Einige Versionen erfordern ein Update für eine AWS Control Tower Tower-Landezone, und andere Versionen werden automatisch in den Service integriert.

Funktionen und Versionen werden in umgekehrter chronologischer Reihenfolge (die neuesten zuerst) aufgeführt, basierend auf dem Datum, an dem sie der Öffentlichkeit offiziell angekündigt wurden.

Themen

- Januar 2026 - Heute
- Januar 2025 — Dezember 2025
- Januar — Dezember 2024
- Januar — Dezember 2023
- Januar — Dezember 2022
- Januar — Dezember 2021
- Januar — Dezember 2020
- Juni — Dezember 2019

Januar 2026 - Heute

Seit Januar 2026 hat AWS Control Tower die folgenden Updates veröffentlicht:

- Account Factory for Terraform (AFT) unterstützt reine Plananpassungsläufe
- AWS Control Tower ist in der europäischen Sovereign Cloud verfügbar

Account Factory for Terraform (AFT) unterstützt reine Plananpassungsläufe

16. September 2026

(Für die AWS Control Tower Tower-Landezone ist kein Update erforderlich.)

Das AWS Control Tower Tower-Framework zur Kontoanpassung, Account Factory for Terraform (AFT), unterstützt jetzt reine Plananpassungsläufe (schreibgeschützt). Sie können die `plan_only` Eingabe an die `aft-invoke-customizations` Zustandsmaschine weiterleiten, um eine

Vorschau der Terraform-Änderungen anzuzeigen, die ein Konto erhalten würde. Auf diese Weise können Sie die Änderungen überprüfen, ohne sie anzuwenden. AFT läuft `terraform plan` statt `terraform apply` auf allen unterstützten Terraform-Distributionen. AFT kann die JSON-Ausgabe des Plans in einen verschlüsselten Amazon S3 S3-Bucket im AFT-Verwaltungskonto exportieren. Bei der Community Edition-Distribution (Open Source) exportiert AFT die Ausgabe standardmäßig. In Terraform Cloud und Terraform Enterprise erfolgt der Export per Opt-In`aft_plan_output_export_enabled`, und Sie können die Ergebnisse auch in der HCP Terraform Run-Benutzeroberfläche anzeigen.

Weitere Informationen finden Sie unter Kontoanpassungen.

AWS Control Tower ist in der europäischen Sovereign Cloud verfügbar

13. Januar 2026

(Für die AWS Control Tower Tower-Landezone ist kein Update erforderlich.)

AWS Control Tower ist jetzt in der europäischen Sovereign Cloud verfügbar. Weitere Informationen zu AWS Control Tower in der europäischen Sovereign Cloud finden Sie im AWS Control Tower Tower-Benutzerhandbuch für die europäische Sovereign Cloud.

Januar 2025 — Dezember 2025

Seit Januar 2025 hat AWS Control Tower die folgenden Updates veröffentlicht:

- Version 4.0 der AWS Control Tower-Landezone
- AWS Control Tower fügt weitere 279 hinzu AWS Config Steuerungen für Control Catalog
- AWS Control Tower ist in der Region Asien-Pazifik (Neuseeland) verfügbar
- AWS Control Tower unterstützt die automatische Kontoregistrierung
- AWS Control Tower aktualisiert die Python-Version
- AWS Control Tower unterstützt IPv6-Adressen
- Der AWS Control Tower reduziert die Drift

  Account Factory für Terraform Version 1.15.0 verfügbar
- Die Steuerelemente mit Nitro-Instanztypen wurden aktualisiert
- AWS Control Tower ist in der Region Asien-Pazifik (Taipeh) verfügbar
- AWS Control Tower unterstützt PrivateLink

- Unterstützung für zusätzliche Branchen-Frameworks, aktualisierte Metadaten
- Service-linked AWS Config Steuerelemente
- Die Konsolenansicht mit aktivierten Steuerelementen bietet eine zentrale Übersicht
- the section called “Account Factory for Terraform (AFT) unterstützt neue Konfigurationen bei der Bereitstellung”
- AWS Control Tower führt Berichte auf Kontoebene für Basis-APIs ein
- the section called “AWS Control Tower ist verfügbar in AWS Regionen Asien-Pazifik (Thailand) und Mexiko (Zentral)”
- Zusätzliche AWS Config Steuerungen verfügbar
- Heben Sie die Registrierung von Aktionen für Organisationseinheiten auf und löschen Sie sie
- the section called “Control Catalog unterstützt IPv6-Adressen”

Version 4.0 der AWS Control Tower-Landezone

17. November 2025

(Für die Landing Zone des AWS Control Tower auf Version 4.0 ist ein Update erforderlich. Weitere Informationen finden Sie unterAktualisiere deine landing zone).

Die AWS Control Tower Landing Zone 4.0 ist ein wichtiges Update, das ein flexibles Controls-Only Erlebnis bietet und es Kunden ermöglicht, die Implementierung und Verwaltung ihrer AWS-Umgebung mit mehreren Konten individuell anzupassen. Diese Version ändert erheblich die Art und Weise, wie AWS Control Tower in AWS-Services integriert wird und organisatorische Ressourcen verwaltet. Informationen zu den wichtigsten Änderungen finden Sie unterLeitfaden zur Migration von Landing Zone v4.0.

Die wichtigsten Änderungen und Funktionen

- Optionale Serviceintegrationen — Mit Landing Zone 4.0 können Sie wählen, welche Serviceintegrationen Sie in Ihrer Umgebung aktivieren möchten. Durch das Deaktivieren einer Integration werden die vom AWS Control Tower bereitgestellten Ressourcen, die für diese Integration spezifisch sind, in den verwalteten Konten und den zentralen Konten der Serviceintegration bereinigt. Sie können Serviceintegrationen jetzt wahlweise aktivieren oder deaktivieren:
  - AWS Config
  - AWS CloudTrail

  - Rollen im Bereich Sicherheit
  - AWS Backup

Wichtig: Wenn Sie die AWS Config-Integration deaktivieren möchten, müssen Sie auch die Integrationen von Security Roles, IAM Identity Center und AWS Backup deaktivieren.

- Dedizierte Ressourcen statt gemeinsam genutzter Ressourcen — Landing Zone 4.0 erstellt jetzt dedizierte Ressourcen für wichtige Dienste. Diese Trennung sorgt für eine bessere Ressourcenisolierung und eine detailliertere Kontrolle über dienstspezifische Ressourcen:
  - Separate S3-Buckets für AWS Config
  - Separate S3-Buckets für AWS CloudTrail
  - Individuelle SNS-Themen für jeden Service

- Flexible Organisationsstruktur — mit Landing Zone 4.0 entfallen die bisherigen Anforderungen an die Organisationsstruktur:
  - Sie müssen keine Sicherheits-OU mehr verwenden
  - Sie können Ihre eigene Organisationsstruktur definieren
  - Die einzige Voraussetzung ist, dass sich alle Hub-Konten in derselben Organisationseinheit befinden müssen
- Erfahrung mit dedizierter Steuerung — Sie können jetzt ein minimales Landezonen-Setup erstellen, das Folgendes beinhaltet:
  - Grundlegende Integration von AWS Organizations
  - Möglichkeit, Steuerungen zu aktivieren, ohne die `AWSControlTowerBaseline` Basislinie zu aktivieren
  - Maßgeschneiderte Governance-Konfigurationen, die auf Ihre Bedürfnisse zugeschnitten sind
- AWS Config Changes — Landing Zone 4.0 führt mehrere Verbesserungen der Implementierung der AWS Config-Integration ein:
  - Eine neue Config-Spoke-Basisversion speziell für Detektivkontrollen
  - Service-linked Config-Aggregator (SLCA) im Config-Hub-Konto
  - Ablösung traditioneller Organisations- und Kontoaggregatoren
- Optionales Manifest:
  - Das Manifestfeld ist jetzt optional und ermöglicht Ihnen:

- Erstellen Sie Landezonen ohne Serviceintegrationen
- Mehr Flexibilität bei der Ersteinrichtung
- Maßgeschneiderte Bereitstellungsoptionen

AWS Control Tower fügt weitere 279 hinzu AWS Config Steuerungen für Control Catalog

14. November 2025

(Für die Landezone des AWS Control Tower ist kein Update erforderlich.)

Der AWS Control Tower enthält jetzt weitere 279 AWS Config Steuerungen als Teil des Control-Katalogs. Sie können die Steuerelemente in der AWS Control Tower-Konsole und über die APIs einsehen.

Bestimmte Steuerelemente haben Beziehungen zu anderen Steuerelementen. Diese Beziehungen werden auch in der AWS Control Tower-Konsole und in den APIs ausgedrückt. Zu den Beziehungstypen gehören „Ergänzend“, „Gegenseitig ausschließen“ und „Alternative“.

AWS Control Tower ist in der Region Asien-Pazifik (Neuseeland) verfügbar

28. Oktober 2025

(Für die Landezone des AWS Control Tower ist kein Update erforderlich.)

AWS Control Tower ist jetzt in der Region Asien-Pazifik (Neuseeland) verfügbar.

Eine vollständige Liste der Regionen, in denen AWS Control Tower verfügbar ist, finden Sie AWS in der Regionentabelle.

AWS Control Tower unterstützt die automatische Kontoregistrierung

15. Oktober 2025

(Für die Landezone des AWS Control Tower ist kein Update erforderlich.)

Für Kunden, die die AWS Control Tower-Landing Zone Version 3.1 oder höher verwenden, ermöglicht AWS Control Tower jetzt die automatische Registrierung von Konten bei OUs. Wenn Sie sich für die automatische Registrierung von Konten entscheiden, wendet AWS Control Tower die für

eine Organisationseinheit aktivierten Basisressourcen und -kontrollen auf ein Konto an, wenn Sie es in eine neue Organisationseinheit verschieben. Kontrollen und Basislinien aus der vorherigen OU werden entfernt. In den meisten Fällen entsteht durch diese Aktion kein Drift.

Um die automatische Registrierung zu aktivieren: Sie können die automatische Registrierung von Konten auf der Seite mit den Landing Zone-Einstellungen in der AWS Control Tower-Konsole auswählen oder indem Sie den AWS Control Tower oder die `UpdateLandingZone` APIs aufrufen, wobei der Wert des `CreateLandingZone` `RemediationType` Parameters auf Inheritance Drift gesetzt ist.

So wenden Sie die automatische Registrierung an: Nachdem Sie diese Option auf Ihrer Einstellungsseite ausgewählt haben, können Sie ein Konto mithilfe der Konsole, der API oder der AWS Control AWS Organizations Tower-Konsole verschieben. AWS Organizations `MoveAccount`

So heben Sie die Registrierung eines Kontos mit automatischer Registrierung auf: Wenn Sie ein Konto außerhalb einer registrierten Organisationseinheit verschieben, entfernt AWS Control Tower automatisch alle bereitgestellten Basisressourcen und Kontrollen.

Weitere Informationen zur automatischen Registrierung finden Sie unter. Konfigurieren Sie optional die automatische Registrierung für Konten

Diese Version enthält auch ein Update für eine verwaltete Richtlinie und eine neue verwaltete Richtlinie. Wir haben das aktualisiert AWS ControlTowerServiceRolePolicy und das Neue hinzugefügt AWS ControlTowerIdentityCenterManagementPolicy.

Wir haben den AWS Control Tower `CreateLandingZone` und die `UpdateLandingZone` APIs aktualisiert`RemediationType`, um einen neuen namens hinzuzufügen`Inheritance Drift`.

AWS Control Tower aktualisiert die Python-Version

3. September 2025

(Für die AWS Control Tower-Landezone ist kein Update erforderlich.)

Python-Version 3.9 ist veraltet. AWS Control Tower hat die Python-Versionen in Ihren AWS Control Tower-Umgebungen aktualisiert. Es sind keine Maßnahmen erforderlich, und dieses Update wirkt sich nicht auf Ihre vorhandenen Workloads aus.

Der AWS Control Tower reduziert die Drift

20. August 2025

(Für die AWS Control Tower-Landezone ist kein Update erforderlich.)

AWS Control Tower hat die Funktionalität von Service Control Policy (SCP) Drift aktualisiert. In dieser Version werden zwei Arten von Governance-Abweichungen direkt vom AWS Control Tower behandelt und führen nicht mehr zu Abweichungen in Ihrer Umgebung.

Zwei Arten von Governance-Drifts wurden beseitigt

- SCP an verwaltete OU angehängt — Diese Art von Drift trat auf, wenn ein SCP für eine Kontrolle an eine andere OU angehängt wurde. Dieses Ereignis trat besonders häufig auf, wenn Sie OUs von außerhalb der AWS Control Tower-Konsole aktualisierten.
- Dem Mitgliedskonto zugeordneter SCP — Diese Art von Abweichung trat häufig auf, wenn ein SCP für eine Kontrolle von außerhalb der AWS Control Tower-Konsole mit einem Konto verknüpft wurde.

Weitere Informationen zu Drift finden Sie unter Drift im AWS Control Tower erkennen und beheben.

AWS Control Tower unterstützt IPv6-Adressen

18. August 2025

(Für die Landezone des AWS Control Tower ist kein Update erforderlich.)

Die AWS Control Tower-API unterstützt jetzt IPv6-Adressen (Internet Protocol Version 6) über unsere neuen Dual-Stack-Endpunkte. Die vorhandenen Endpunkte, die IPv4 unterstützen, bleiben aus Gründen der Abwärtskompatibilität verfügbar. Die neuen Dual-Stack-Domains sind entweder über das Internet oder über eine Amazon Virtual Private Cloud (VPC) verfügbar. AWS PrivateLink

Account Factory für Terraform Version 1.15.0 verfügbar

28. Juli 2025

(Für die AWS Control Tower-Landezone ist kein Update erforderlich.)

Version 1.15.0 von AWS Control Tower Account Factory für Terraform (AFT) ist verfügbar. Weitere Informationen finden Sie im AFT-Repository. GitHub

Die Steuerelemente mit Nitro-Instanztypen wurden aktualisiert

24. Juli 2025

(Für die AWS Control Tower-Landezone ist kein Update erforderlich.)

AWS Control Tower hat die acht proaktiven Kontrollen im Control Catalog (früher Control Library genannt) aktualisiert, die die Amazon EC2-Instance-Typen durchsetzen. Dieses Update ermöglicht es Ihnen, einige neue Nitro-Instance-Typen zu instanziieren, und es entfernt einige veraltete Instance-Typen der U-Serie.

Die Steuerelemente wurden aktualisiert

- CT.AUTOSCALING.PR.10
- CT.AUTOSCALING.PR.11
- CT.EC2.PR.15
- CT.EC2.PR.16
- CT.EC2.PR.17
- CT.EC2.PR.18
- CT.EC2.PR.19
- CT.EC2.PR.20

Neue Instance-Typen verfügbar

- c8gd
- c8gn
- i7i
- m8gd
- p6-b200
- r8gd

Instanztypen wurden entfernt

- u-12tb1
- u-18tb1
- u-24tb1
- u-9tb1

Die aktualisierten Steuerelemente sind überall dort verfügbar AWS-Regionen , wo AWS Control Tower verfügbar ist. Eine Liste der Regionen, in denen AWS Control Tower verfügbar ist, finden Sie in der AWS-Region Tabelle.

AWS Control Tower ist in der Region Asien-Pazifik (Taipeh) verfügbar

23. Juli 2025

(Für die AWS Control Tower-Landezone ist kein Update erforderlich.)

AWS Control Tower ist jetzt in der Region Asien-Pazifik (Taipeh) verfügbar:

Eine vollständige Liste der Regionen, in denen AWS Control Tower verfügbar ist, finden Sie AWS in der Regionentabelle.

AWS Control Tower unterstützt PrivateLink

30. Juni 2025

(Für die AWS Control Tower-Landezone ist kein Update erforderlich.)

AWS Control Tower unterstützt jetzt AWS PrivateLink. Sie können die APIs AWS Control Tower und Control Catalog von Ihrer Amazon Virtual Private Cloud (VPC) aus aufrufen, ohne das öffentliche Internet zu nutzen. AWS PrivateLink bietet private Konnektivität zwischen Virtual Private Clouds (VPCs), unterstützten Diensten und Ressourcen sowie Ihren lokalen Netzwerken. AWS PrivateLink Unterstützung für AWS Control Tower ist überall dort verfügbar, AWS-Regionen wo AWS Control Tower verfügbar ist.

Unterstützung für zusätzliche Branchen-Frameworks, aktualisierte Metadaten

12. Juni 2025

(Für die AWS Control Tower-Landezone ist kein Update erforderlich.)

Mit dieser Version wird der AWS Control Tower um die Unterstützung von 10 branchenspezifischen Frameworks erweitert. Eine Liste der Frameworks finden Sie unter Unterstützte Frameworks.

Sie können beispielsweise beginnen, indem Sie in der AWS Control Tower-Konsole zur Control Catalog-Seite navigieren und nach einem Framework suchen, z. B. um alle Kontrollen zu sehen PCI-DSS-v4.0, die sich auf dieses Framework beziehen. Oder Sie können Kontrollen und Frameworks programmgesteuert untersuchen, indem Sie die neue API aufrufen. `ListControlMappings`

Die mit Steuerelementen verknüpften Metadatendefinitionen ändern sich, um diese zusätzlichen branchenspezifischen Frameworks besser zu unterstützen. Die Änderungen an den Metadaten können sich auf die Art und Weise auswirken, wie Sie Steuerelemente im Hinblick auf ihre Aktivierung evaluieren. Beispielsweise könnten sich die Werte für NIST-, PCI- und CIS-Metadaten geändert haben. Wir empfehlen Ihnen, die Zuordnungen für Ihre aktivierten Steuerelemente auf der Seite mit den Kontrolldetails in der Konsole zu überprüfen.

In der Konsole und der API haben wir 3 neue Metadatenfelder eingeführt. Zusammengenommen beschreiben diese Felder eine Hierarchie, anhand derer Sie besser verstehen, wie Steuerelemente kategorisiert und aktiviert werden. Die Felder sind: Domain , Objective und Common Control . Wir haben unsere Kontrollziele neu definiert, um sie besser an den breiteren Anwendungsbereich der verfügbaren branchenspezifischen Rahmenbedingungen anzupassen. Weitere Informationen zu dieser Hierarchie finden Sie unter Ontologie-Überblick.

- Diese Metadatenänderungen werden in der AWS Control Tower-Konsole wiedergegeben, und die Konsolenerfahrung ist im gesamten AWS Control Tower und auf den AWS Config Konsolen einheitlich.
- Um Kontrollinformationen in der AWS Control Tower-Konsole anzuzeigen, müssen Sie Ihren IAM-Richtlinien zusätzliche `controlcatalog` Berechtigungen hinzufügen. Weitere Informationen finden Sie unter Für die Verwendung der AWS Control Tower-Konsole erforderliche Berechtigungen.
- Jedes Steuerelement hat jetzt ein neues Feld namens`GovernedResources`, das die Ressourcentypen anzeigt, für die das Steuerelement zuständig ist. In einigen Fällen zeigt dieses Feld das Dienstpräfix für die Ressourcen an, in anderen Fällen kann es leer sein. Weitere Informationen erhalten Sie unter `GetControl` und `ListControls`.

In dieser Version haben wir die Controls Library aus Gründen der Konsistenz mit anderen Begriffen in Control Catalog umbenannt.

Service-linked AWS Config Steuerelemente

12. Juni 2025

(Für die AWS Control Tower-Landezone ist kein Update erforderlich.)

AWS Control Tower kündigt an, dass die AWS Control Tower Detective Controls in Form von serviceverknüpften AWS Config Regeln unterstützt werden.

Mit dieser Version stellt AWS Control Tower nun serviceverknüpfte Config-Regeln direkt in Ihren registrierten Konten bereit und ersetzt so die bisherige Bereitstellungsmethode durch Stack-Sets. AWS CloudFormation Diese Änderung verbessert die Bereitstellungsgeschwindigkeit erheblich. Außerdem tragen diese dienstbezogenen Config-Regeln dazu bei, eine konsistente Verwaltung Ihrer Ressourcen zu gewährleisten, da sie unbeabsichtigte Konfigurationsabweichungen verhindern, die durch manuelle Änderungen an CloudFormation Stack-Sets oder Config-Regeln verursacht werden könnten.

In Zukunft werden alle durch AWS Config Regeln implementierten AWS Control Tower-Kontrollen mit diesem Mechanismus bereitgestellt, der die APIs direkt aufruft. AWS Config

> **Important**
>
> Bevor Sie serviceverknüpfte Config-Regeln übernehmen, überprüfen Sie die vorhandenen Anpassungen, z. B. Korrekturen, die Sie außerhalb von AWS Control Tower an den Config-Regeln vorgenommen haben, da diese Anpassungen während der Umstellung entfernt werden. Die AWS Config APIs unterstützen nicht das Hinzufügen von Behebungskonfigurationen für serviceverknüpfte Regeln. AWS Config Siehe `PutRemediationConfigurations`.

Details und Maßnahmen erforderlich

- Wenn Sie Ihre Landezone aktualisieren oder zurücksetzen, aktualisiert AWS Control Tower die obligatorischen Kontrollen, die die Sicherheits-OU regeln. Um das Upgrade abzuschließen, müssen Sie außerdem alle Detective Controls, die mit AWS Config Regeln implementiert sind, oder Re-register die OU zurücksetzen.
- Der volle Umfang dieses Upgrades gilt für Sie, wenn Ihre AWS Control Tower Landing Zone-Version 3.2 oder höher ist. Wenn Sie dieses Update anwenden, werden Ihre vorhandenen AWS Config Regeln zusammen mit der neuen Bereitstellungsmethode in service-verwaltete Config-Regeln geändert.
- Wenn Ihre Landing Zone Version 3.1 oder niedriger ist, werden alle neuen Config-Regeln mit der neuen Methode bereitgestellt, nicht mehr mit Stack-Sets. Deine bestehenden Config-Regeln werden NICHT aktualisiert, sodass sie zu dienstverwalteten Config-Regeln werden. Sie bleiben vom Standardtyp.
- Sie können dienstgebundene Konfigurationsregeln anhand ihrer Ressourcen-ARN identifizieren, die das folgende Format hat:

```
arn:aws:config:*:*:config-rule/aws-service-rule/controltower.*/*
```

Die beabsichtigte Funktionalität von Steuerelementen, wenn sie durch dienstgebundene AWS Config Regeln implementiert werden, hat sich nicht geändert. Mithilfe der serviceverknüpften Config-Regeln von Detective im AWS Control Tower können Ressourcen in Ihren Konten identifiziert werden, die nicht den Richtlinien entsprechen, und über das Dashboard Warnmeldungen ausgeben. Um die Konsistenz zu wahren, Konfigurationsabweichungen zu vermeiden und Ihre allgemeine Benutzererfahrung zu vereinfachen, können diese Regeln jetzt nur noch über AWS Control Tower geändert werden.

Im Rahmen dieser Version haben wir der Richtlinie für die serviceverknüpfte Rolle (SLR) vier neue Berechtigungen hinzugefügt `AWSServiceRoleForAWSControlTower`, sodass Sie serviceverknüpfte AWS Config Regeln für Ihre registrierten Konten aktivieren und deaktivieren können.

```
config:DescribeConfigRules
config:TagResource
config:PutConfigRule
config:DeleteConfigRule
```

Die Konsolenansicht mit aktivierten Steuerelementen bietet eine zentrale Übersicht

21. Mai 2025

(Für die AWS Control Tower-Landezone ist kein Update erforderlich.)

AWS Control Tower hat der Konsole eine neue Seite hinzugefügt, auf der alle Ihre aktivierten Steuerelemente in einer einzigen, zentralen Ansicht angezeigt werden. Bisher waren Steuerelemente nur mit dem Konto oder der OU sichtbar, auf dem sie aktiviert waren. Die konsolidierte Ansicht erleichtert es Ihnen, Lücken in Ihrer Kontrollverwaltung in großem Maßstab zu identifizieren.

Auf der Seite Aktivierte Kontrollen können Sie die Kontrollen nach Verhalten filtern: Präventiv, Detektiv oder Proaktiv. Sie können auch nach der Implementierung der Kontrollelemente filtern, z. B. nach SCP. Für jedes Steuerelement können Sie sehen, für wie viele Organisationseinheiten dieses Steuerelement aktiviert ist.

Um die Seite „Aktivierte Steuerelemente“ aufzurufen, navigieren Sie zum Abschnitt „Kontrollen“ in der AWS Control Tower-Konsole.

Account Factory for Terraform (AFT) unterstützt neue Konfigurationen bei der Bereitstellung

13. Mai 2025

(Für die AWS Control Tower-Landezone ist kein Update erforderlich.)

Das AWS Control Tower-Framework zur Kontoanpassung, Account Factory for Terraform (AFT), unterstützt jetzt drei zusätzliche optionale Konfigurationen zum Zeitpunkt der Bereitstellung. Sie können AFT in einer benutzerdefinierten Virtual Private Cloud (VPC) bereitstellen, den Terraform-Projektnamen für Ihre AFT-Bereitstellung angeben und die von AFT erstellten Ressourcen taggen.

Weitere Informationen finden Sie unter Bereitstellen von AWS Control Tower Account Factory für Terraform (AFT).

AWS Control Tower führt Berichte auf Kontoebene für Basis-APIs ein

12. Mai 2025

(Für die AWS Control Tower-Landezone ist kein Update erforderlich.)

Sie können jetzt den Status der Drift und der Kontoregistrierung für Ihre verwalteten Konten programmgesteuert einsehen, indem Sie die Basis-APIs aufrufen. Mit dieser Funktion können Sie feststellen, wann die Basiskonfigurationen von Konto und Organisationseinheit abweichen oder nicht mehr synchron sind. Um den Drift-Status programmgesteuert anzuzeigen, können Sie die `ListEnabledBaselines` API für Ihre aktivierten Baselines aufrufen. Verwenden Sie das Flag, um den Status einzelner Konten programmgesteuert mit der API anzuzeigen. `ListEnabledBaselines` `includeChildren` Sie können nach diesen Status filtern und nur die Konten und Organisationseinheiten sehen, die Ihre Aufmerksamkeit erfordern.

Das `AWS ControlTowerBaseline` richtet Best-Practice-Konfigurationen, Kontrollen und Ressourcen ein, die für die Verwaltung erforderlich sind. Wenn Sie diese Baseline für eine Organisationseinheit (OU) aktivieren, werden Mitgliedskonten innerhalb der OU automatisch bei AWS Control Tower registriert. Die grundlegenden APIs von AWS Control Tower beinhalten CloudFormation Support, der es Ihnen ermöglicht, Automatisierungen zu erstellen, mit denen Sie Ihre Organisationseinheiten und Konten mit Infrastructure as Code (IaC) verwalten können.

Weitere Informationen zu diesen APIs finden Sie in den Baselines im AWS Control Tower-Benutzerhandbuch. Die grundlegenden APIs und die neu eingeführten Berichtsfunktionen für den Drift - und Kontoregistrierungsstatus sind überall dort verfügbar, AWS-Regionen wo AWS Control Tower verfügbar ist. Eine Liste der Standorte AWS-Regionen , an denen AWS Control Tower verfügbar ist, finden Sie in der AWS-Region Tabelle.

AWS Control Tower ist verfügbar in AWS Regionen Asien-Pazifik (Thailand) und Mexiko (Zentral)

9. Mai 2025

(Für die Landezone des AWS Control Tower ist kein Update erforderlich.)

AWS Control Tower ist jetzt in den folgenden AWS Regionen verfügbar:

- Asien-Pazifik (Thailand)
- Mexiko (Zentral)

Eine vollständige Liste der Regionen, in denen AWS Control Tower verfügbar ist, finden Sie AWS in der Regionentabelle.

Zusätzliche AWS Config Steuerungen verfügbar

11. April 2025

(Für die AWS Control Tower-Landezone ist kein Update erforderlich.)

AWS Control Tower unterstützt jetzt weitere 223 verwaltete AWS Config Regeln für verschiedene Anwendungsfälle wie Sicherheit, Kosten, Haltbarkeit und Betrieb. Mit dieser Einführung können Sie jetzt AWS Control Tower verwenden, um die AWS Config Regeln zu suchen und zu ermitteln, die Sie zur Steuerung Ihrer Umgebung mit mehreren Konten benötigen. Anschließend können Sie die Kontrollen direkt vom AWS Control Tower aus aktivieren und verwalten.

Um von der AWS Control Tower-Konsole aus zu beginnen, gehen Sie zum Control Catalog und suchen Sie mit dem Implementierungsfilter nach Steuerelementen AWS Config. Sie können die Steuerungen direkt von der AWS Control Tower-Konsole aus aktivieren.

Weitere Informationen finden Sie unter Integrierte AWS Config Steuerelemente, die im AWS Control Tower verfügbar sind.

Mit dieser Markteinführung haben wir die `GetControl` APIs `ListControls` und aktualisiert, um drei neue Felder zu unterstützen: CreateTime Schweregrad und Implementierung. Diese Felder können Sie verwenden, wenn Sie im Control Catalog nach einer Kontrolle suchen. Beispielsweise können Sie jetzt programmgesteuert nach AWS Config Regeln mit hohem Schweregrad suchen, die nach Ihrer letzten Bewertung erstellt wurden.

Sie können überall dort, AWS-Regionen wo AWS Control Tower verfügbar ist, nach den neuen AWS Config Regeln suchen. Um eine Regel bereitzustellen, sehen Sie in der Liste der unterstützten AWS-Regionen Regeln nach, wo sie aktiviert werden kann.

Heben Sie die Registrierung von Aktionen für Organisationseinheiten auf und löschen Sie sie

8. April 2025

(Für die AWS Control Tower-Landezone ist kein Update erforderlich.)

AWS Control Tower unterstützt jetzt separate Konsolenaktionen zum Deregistrieren einer OU und zum Löschen einer OU. Sie müssen die OU deregistrieren, bevor Sie sie löschen. Sie können eine OU aus dem AWS Control Tower entfernen, indem Sie sie abmelden.

Weitere Informationen finden Sie unter Eine Organisationseinheit entfernen.

Control Catalog unterstützt IPv6-Adressen

2. April 2025

(Für die Landezone des AWS Control Tower ist kein Update erforderlich.)

Die AWS Control Tower Control Catalog API unterstützt jetzt IPv6-Adressen (Internet Protocol Version 6) über unsere neuen Dual-Stack-Endpunkte. Die bestehenden Control Catalog-Endpunkte, die IPv4 unterstützen, sind aus Gründen der Abwärtskompatibilität weiterhin verfügbar. Die neuen Dual-Stack-Domains sind entweder über das Internet oder innerhalb einer Amazon Virtual Private Cloud (VPC) unter Verwendung von Amazon verfügbar. AWS PrivateLink

Januar — Dezember 2024

Im Jahr 2024 veröffentlichte AWS Control Tower die folgenden Updates:

- AWS Control Tower CFCT unterstützt GitHub und RCPs
- AWS Control Tower fügt präventive Kontrollen mit deklarativen Richtlinien hinzu
- AWS Control Tower bietet Optionen für präskriptive Backup-Pläne
- AWS Control Tower ist integriert AWS Config Steuerelemente
- AWS Control Tower verbessert das Hook-Management und fügt proaktive Kontrollregionen hinzu
- AWS Control Tower führt Richtlinien für die Verwaltung von Ressourcen ein
- AWS Control Tower meldet eine Abweichung der Kontrollrichtlinien
- Neue `ResetEnabledControl` API
- `GetControl`API zur Steuerung von Katalogaktualisierungen
- AWS Control Tower AFT unterstützt GitLab
- AWS Control Tower ist verfügbar in AWS Asien-Pazifik (Malaysia)
- AWS Control Tower unterstützt bis zu 1000 Konten pro OU
- AWS Control Tower fügt eine Versionsauswahl für die Landezone hinzu
- Beschreibende Kontroll-API verfügbar, erweiterter Zugriff auf Regionen und Steuerelemente
- AWS Control Tower unterstützt AFT und cFCT in Opt-in-Regionen
- AWS Control Tower fügt die `ListLandingZoneOperations` API hinzu
- AWS Control Tower unterstützt bis zu 100 gleichzeitige Kontrollvorgänge
- AWS Control Tower ist verfügbar in AWS Kanada West (Calgary)
- AWS Control Tower unterstützt Self-Service-Kontingentanpassungen
- AWS Control Tower veröffentlicht den Referenzhandbuch für Steuerungen
- AWS Control Tower aktualisiert zwei proaktive Kontrollen und benennt sie um
- Veraltete Steuerelemente sind nicht mehr verfügbar
- AWS Control Tower unterstützt das Taggen von `EnabledControl` Ressourcen in CloudFormation
- AWS Control Tower unterstützt APIs für die Registrierung und Konfiguration von Organisationseinheiten mit Baselines

AWS Control Tower CFCT unterstützt GitHub und RCPs

9. Dezember 2024

(Für die Landezone des AWS Control Tower ist kein Update erforderlich.)

AWS Control Tower unterstützt jetzt GitHub TM ™ als Option für ein Versionskontrollsystem (VCS) eines Drittanbieters und als Konfigurationsquelle für Anpassungen für AWS Control Tower (CFCT). Weitere Informationen finden Sie unter GitHub Als Konfigurationsquelle einrichten.

AWS Control Tower unterstützt jetzt Resource Control Policies (RCPs) für Anpassungen für AWS Control Tower (CFCT). Weitere Informationen finden Sie unter Leitfaden zur cFCT-Anpassung.

AWS Control Tower fügt präventive Kontrollen mit deklarativen Richtlinien hinzu

1. Dezember 2024

(Für die Landezone des AWS Control Tower ist kein Update erforderlich.)

AWS Control Tower unterstützt jetzt präventive Kontrollen, die durch deklarative Richtlinien von AWS Organizations implementiert werden. Deklarative Richtlinien werden direkt auf Serviceebene angewendet. Dieser Ansatz stellt sicher, dass die angegebene Konfiguration auch dann durchgesetzt wird, wenn der Dienst neue Funktionen oder APIs einführt. Weitere Informationen finden Sie unter Mit deklarativen Richtlinien implementierte Steuerelemente.

AWS Control Tower bietet Optionen für präskriptive Backup-Pläne

25. November 2024

(Für die Landezone des AWS Control Tower ist kein Update erforderlich.)

AWS Control Tower unterstützt jetzt verbindliche AWS Backup Pläne, mit denen Sie einen Workflow zur Datensicherung und -wiederherstellung direkt in Ihre Landezone integrieren können. Der Backup-Plan beinhaltet vordefinierte Regeln wie Aufbewahrungstage, Sicherungshäufigkeit und das Zeitfenster, in dem die Sicherung erfolgt. Diese Regeln definieren, wie Sie Ihre AWS Ressourcen auf all Ihren verwalteten Mitgliedskonten sichern. Wenn Sie einen Backup-Plan auf die Landing Zone anwenden, stellt AWS Control Tower sicher, dass der Plan für alle Mitgliedskonten einheitlich ist und den Empfehlungen von AWS Backup zu bewährten Methoden entspricht.

Weitere Informationen finden Sie unter AWS Backup und AWS Control Tower.

AWS Control Tower ist integriert AWS Config Steuerelemente

21. November 2024

(Für die Landezone des AWS Control Tower ist kein Update erforderlich.)

AWS Control Tower hat ausgewählte AWS Config Steuerelemente integriert, sodass sie vom AWS Control Tower eingesehen und verwaltet werden können.

Weitere Informationen finden Sie unter Integrierte AWS Config Steuerelemente, die in AWS Control Tower verfügbar sind

AWS Control Tower verbessert das Hook-Management und fügt proaktive Kontrollregionen hinzu

20. November 2024

(Für die Landezone des AWS Control Tower ist kein Update erforderlich.)

Mit dieser Version können Sie die volle Kapazität der CloudFormation Hooks nutzen, ohne dass dies durch AWS Control Tower eingeschränkt wird. Proaktive Kontrollen sind auch in den Regionen Kanada West (Calgary) und Asien-Pazifik (Malaysia) verfügbar.

Bisher mussten alle CloudFormation Hooks in Ihrer Umgebung durch die CT.CLOUDFORMATION.PR.1 Steuerung geschützt werden, sodass nur AWS Control Tower sie ändern konnte. Mit dieser Version können Sie CloudFormation Hooks bereitstellen und diese Hooks ändern, ohne die Einschränkungen, die zuvor für den AWS Control Tower-Service erforderlich waren.

Wenn Sie derzeit proaktive Kontrollen einsetzen, können Sie auf diese verbesserte Hook-Funktionalität umsteigen. Um alle proaktiven Steuerungen in einer Organisationseinheit zurückzusetzen, setzen Sie jedes einzelne proaktive Steuerelement zurück, das auf dieser Organisationseinheit aktiv ist. Sie können den Reset durchführen, indem Sie die `ResetEnabledControl` API aufrufen oder das Steuerelement mithilfe der Reset-Funktion von der Konsole aus aktualisieren. Wenn Sie diese Reset-Aufgabe für eine proaktive Steuerung abgeschlossen haben, verschiebt AWS Control Tower alle proaktiven Kontroll-Hooks auf der OU auf die neue Funktion. Wiederholen Sie diesen Vorgang für jede Organisationseinheit, die proaktive Kontrollen einsetzt.

Nachdem Sie eine proaktive Steuerung zurückgesetzt haben, entfernen Sie die CT.CLOUDFORMATION.PR.1 Kontrolle auf Ihren AWS Control Tower-OUs, sofern Sie diese Steuerung nicht für einen anderen Zweck aktiviert haben. Wenn Sie die CT.CLOUDFORMATION.PR.1 Steuerung nicht ausschalten, können Sie Ihre anderen CloudFormation Hooks nicht erstellen und ändern.

Weitere Informationen finden Sie unter Proaktive Control-Hooks aktualisieren.

AWS Control Tower führt Richtlinien für die Verwaltung von Ressourcen ein

15. November 2024

(Für die Landezone des AWS Control Tower ist kein Update erforderlich.)

AWS Control Tower bietet eine neue Art der präventiven Kontrolle, die mithilfe von Richtlinien zur Ressourcenkontrolle (RCPs) implementiert wird. Diese Kontrollen helfen Ihnen dabei, einen Datenperimeter in Ihrer AWS Control Tower-Umgebung einzurichten, um Ihre Ressourcen vor unbeabsichtigtem Zugriff zu schützen.

Sie können beispielsweise RCP-based Steuerungen für Amazon S3 AWS -Security-Token-Service AWS Key Management Service, Amazon SQS und Services aktivieren. AWS Secrets Manager Eine RCP-based Steuerung kann eine Anforderung wie „Erfordern, dass nur IAM-Prinzipale, die zur Organisation gehören, oder ein AWS Service auf die Amazon S3-Ressourcen der Organisation zugreifen können“ durchsetzen, unabhängig von den Berechtigungen, die für einzelne Bucket-Richtlinien gewährt wurden.

Sie können die neuen RCP-based Kontrollen und bestimmte vorhandene SCP-based präventive Kontrollen so konfigurieren, dass AWS IAM-Ausnahmen für Principals und Ressourcen festgelegt werden. Wenn Sie nicht möchten, dass ein Hauptbenutzer oder eine Ressource der Kontrolle unterliegt, können Sie eine Ausnahme konfigurieren.

Durch die Kombination von präventiven, proaktiven und detektivischen Kontrollen im AWS Control Tower können Sie überwachen, ob Ihre AWS Umgebung mit mehreren Konten sicher ist und gemäß bewährten Methoden wie dem AWS Foundational Security Best Practices-Standard verwaltet wird.

Diese neuen RCP-based präventiven Kontrollen sind dort verfügbar AWS-Regionen , wo AWS Control Tower verfügbar ist. Eine vollständige Liste der Standorte AWS-Regionen , an denen AWS Control Tower verfügbar ist, finden Sie in der AWS-Region Tabelle.

AWS Control Tower meldet eine Abweichung der Kontrollrichtlinien

15. November 2024

(Für die Landezone des AWS Control Tower ist kein Update erforderlich.)

AWS Control Tower meldet jetzt Abweichungen von den Kontrollrichtlinien für Kontrollen, die mit Resource Control Policies (RCPs) implementiert wurden, und für Kontrollen, die Teil des Security

Hub Service-managed CSPM-Standards sind: AWS Control Tower. Diese Art von Abweichung kann durch die neue API behoben werden. `ResetEnabledControl` Weitere Informationen finden Sie unter Arten von Governance-Abweichungen.

Neue **`ResetEnabledControl`** API

14. November 2024

(Für die Landezone des AWS Control Tower ist kein Update erforderlich.)

AWS Control Tower kündigt eine neue API an, mit der Sie Kontrollabweichungen programmgesteuert verwalten können. Sie können die Kontrollabweichung reparieren und eine Steuerung auf die vorgesehene Konfiguration zurücksetzen. Die `ResetEnabledControl` API funktioniert mit optionalen AWS Control Tower-Steuerelementen, einschließlich der Steuerelemente „Strong Recommended“ und „Elective“.

Kontrollieren Sie Ausnahmen

- Kontrollen, die mit Service Control Policies (SCPs) implementiert wurden, können mit dieser API nicht zurückgesetzt werden. Weitere Informationen finden Sie unter `ResetEnabledControl`.
- Obligatorische Kontrollen können nicht zurückgesetzt werden, da sie die Ressourcen des AWS Control Tower schützen.
- Die Region, die die Kontrolle über die Landezone verweigert, muss über die Konsole zurückgesetzt werden.

Eine Kontrollabweichung tritt auf, wenn eine AWS-Control-Tower-Steuerung außerhalb des AWS Control Tower geändert wird, beispielsweise von der AWS Organizations Konsole aus. Wenn Sie Abweichungen beheben, können Sie sicherstellen, dass Sie die behördlichen Anforderungen einhalten.

`GetControl`API zur Steuerung von Katalogaktualisierungen

8. November 2024

(Für die Landezone des AWS Control Tower ist kein Update erforderlich.)

AWS Control Tower unterstützt jetzt eine aktualisierte `GetControl` API, die zwei neue Felder enthält: `Implementation` Typen für alle Steuerelemente und `Parameters` für bestimmte Steuerelemente, die konfiguriert werden können.

Die `GetControl` API ist Teil des `controlcatalog` Namespaces von AWS Control Tower.

Weitere Informationen finden Sie unter der `GetControl API` in der Control Catalog API-Referenz.

Diese Version enthält verwandte Änderungen, die in der AWS Control Tower-Konsole angezeigt werden.

- Bei allen vorhandenen AWS Security Hub CSPM Steuerelementen wurde der `Implementation` Parameterwert von AWS Config Regel zu geändert AWS Security Hub CSPM. Das entsprechende Hilfefenster der Konsole wurde geändert, um dieser Änderung Rechnung zu tragen.
- Bei allen vorhandenen Hook-Steuerelementen wurde der `Implementation` Parameterwert von CloudFormation Guard-Regel zu CloudFormation Hook geändert. Das entsprechende Hilfefenster der Konsole wurde geändert, um dieser Änderung Rechnung zu tragen.

AWS Control Tower AFT unterstützt GitLab

23. Oktober 2024

(Für die Landezone des AWS Control Tower ist kein Update erforderlich.)

AWS Control Tower unterstützt jetzt GitLab TM ™ und GitLab Self-managed als Optionen für ein Versionskontrollsystem (VCS) eines Drittanbieters und eine Konfigurationsquelle für Account Factory for Terraform (AFT).

AWS Control Tower ist verfügbar in AWS Asien-Pazifik (Malaysia)

21. Oktober 2024

(Für die Landezone des AWS Control Tower ist kein Update erforderlich.)

AWS Control Tower ist in der Region AWS Asien-Pazifik (Malaysia) verfügbar.

Eine vollständige Liste der Regionen, in denen AWS Control Tower verfügbar ist, finden Sie AWS in der Regionentabelle.

AWS Control Tower unterstützt bis zu 1000 Konten pro OU

30. August 2024

(Für die Landezone des AWS Control Tower ist kein Update erforderlich.)

AWS Control Tower hat die maximal zulässige Anzahl von Konten pro Organisationseinheit (OU) von 300 auf 1000 erhöht. Jetzt können Sie bis AWS-Konten zu 1000 Personen gleichzeitig für AWS Control Tower Governance registrieren, ohne Ihre Organisationsstruktur zu ändern. Die Prozesse zur Registrierung und erneuten Registrierung von Organisationseinheiten sind ebenfalls effizienter und erfordern deutlich weniger Zeit, um die grundlegenden Ressourcen von AWS Control Tower in Ihren Konten bereitzustellen.

Aufgrund der begrenzten Anzahl verfügbarer CloudFormation Stack-Sets gelten weiterhin einige Kontobeschränkungen. Insbesondere die maximale Anzahl von Konten, die Sie für eine OU registrieren können, kann je nach der Anzahl der Regionen, denen Sie unterstehen, unterschiedlich sein. Weitere Informationen finden Sie im AWS Control Tower-Benutzerhandbuch unter Einschränkungen, die auf den zugrunde liegenden AWS Diensten basieren. Eine vollständige Liste der Standorte AWS-Regionen , an denen AWS Control Tower verfügbar ist, finden Sie in der AWS-Region Tabelle.

AWS Control Tower fügt eine Versionsauswahl für die Landezone hinzu

15. August 2024

(Für die Landezone des AWS Control Tower ist kein Update erforderlich.)

Wenn Sie die AWS Control Tower-Landing Zone Version 3.1 und höher verwenden, können Sie Ihre in der aktuellen Version vorhandene Landezone aktualisieren oder reparieren, oder Sie können ein Upgrade auf eine Version Ihrer Wahl durchführen. Bisher war für jede Aktualisierung oder Reparatur der Landing Zone ein Upgrade auf die neueste Version der Landing Zone erforderlich.

Mit der Auswahl der Landing Zone-Version haben Sie mehr Flexibilität bei der Planung von Versions-Upgrades, während Sie mögliche Änderungen an Ihrer Umgebung evaluieren. Sie müssen sich nicht entscheiden, ob Sie Drift reparieren möchten, um die Konformität zu gewährleisten, Ihre Landing Zone-Konfigurationen zu aktualisieren oder ein Upgrade auf die neueste Landing Zone-Version durchzuführen. Wenn du die Landing Zone-Version 3.1 oder höher verwendest, kannst du wählen, ob du die aktuelle Version beibehalten oder auf eine neuere Version upgraden möchtest, wenn du deine Landing Zone-Konfigurationen aktualisierst oder zurücksetzt.

Beschreibende Kontroll-API verfügbar, erweiterter Zugriff auf Regionen und Steuerelemente

6. August 2024

(Für die Landezone des AWS Control Tower ist kein Update erforderlich.)

AWS Control Tower hat zwei neue API-Operationen hinzugefügt, die Ihnen helfen, programmatisch mehr Informationen über verfügbare Steuerelemente zu finden. Diese Funktion erleichtert die automatisierte Bereitstellung von Steuerungen.

- Die `GetControl` API gibt Details zu einer aktivierten Steuerung zurück, einschließlich der Ziel-ID, einer Zusammenfassung der Kontrollinformationen, einer Liste der Zielregionen und des Drift-Status.
- Die `ListControls` API gibt eine paginierte Liste aller verfügbaren Steuerelemente in der Kontrollbibliothek des AWS Control Tower zurück.

Diese APIs werden über den AWS Control Catalog-Namespace erreicht. Der AWS Control Catalog ist Teil von AWS Control Tower, der Steuerelemente enthält, die Sie bei der Verwaltung anderer AWS Dienste unterstützen, nicht nur des AWS Control Tower. Dieser erweiterte Katalog konsolidiert die Steuerelemente verschiedener AWS Services, sodass Sie die AWS Steuerelemente anhand einiger häufiger Anwendungsfälle wie Sicherheit, Kosten, Haltbarkeit und Betrieb einsehen können. Weitere Informationen finden Sie in der Control Catalog API-Referenz.

Erweiterte Verfügbarkeit in der Region

Ab dieser Version können Sie die AWS Control Tower-Governance auf Bereiche ausweiten AWS-Regionen , in denen einige Ihrer (bereits) aktivierten Steuerelemente nicht verfügbar sind. Außerdem können Sie jetzt bestimmte Steuerelemente in mehr Regionen aktivieren, auch wenn die Steuerung nicht in allen Ihren regulierten Regionen unterstützt wird.

Bisher hinderte der AWS Control Tower Sie daran, die Governance auf Regionen auszudehnen oder Kontrollen zu aktivieren, obwohl es nicht für alle Ihre aktivierten Kontrollen und regulierten Regionen konsistent war. Mit dieser Version haben Sie mehr Flexibilität und mehr Verantwortung, um sicherzustellen, dass Ihre Konfiguration für alle aktivierten Kontrollen und alle kontrollierten Regionen korrekt ist. Die Kontroll-APIs und die Kontrollkatalog-APIs von AWS können Ihnen dabei helfen, Informationen über die AWS Regionen zu erhalten, in denen Sie durch aktivierte Kontrollen geschützt sind, und über die Regionen, in denen zusätzliche Kontrollen eingesetzt werden können. Regions- und Kontrollinformationen sind auch in der AWS Control Tower-Konsole verfügbar.

AWS Control Tower unterstützt AFT und cFCT in Opt-in-Regionen

18. Juli 2024

(Für die Landezone des AWS Control Tower ist kein Update erforderlich.)

Heute sind die AWS-Control-Tower-Anpassungsframeworks Account Factory for Terraform (AFT) und Customizations for AWS Control Tower (cFCT) in fünf weiteren Versionen verfügbar AWS-Regionen: Asien-Pazifik (Hyderabad, Jakarta und Osaka), Israel (Tel Aviv) und Naher Osten (VAE).

Account Factory for Terraform (AFT) richtet eine Terraform-Pipeline ein, um Sie bei der Bereitstellung und Anpassung von Konten im AWS Control Tower zu unterstützen. Anpassungen für AWS Control Tower (cFCT) helfen Ihnen dabei, Ihre AWS Control Tower-Landingzone und Konten mithilfe von CloudFormation Vorlagen und Service Control Policies (SCPs) anzupassen.

Weitere Informationen finden Sie auf den Seiten Account Factory for Terraform und Customizations for AWS Control Tower im AWS Control Tower-Benutzerhandbuch. Möglicherweise möchten Sie auch die Versionshinweise auf der AFT Github-Seite und der cFCT Github-Seite lesen. AFT und cFCT werden mit einigen Ausnahmen in allen AWS Regionen unterstützt. Einzelheiten finden Sie unter Regionsbeschränkungen.

AWS Control Tower fügt die **`ListLandingZoneOperations`** API hinzu

26. Juni 2024

(Für die Landezone des AWS Control Tower ist kein Update erforderlich.)

AWS Control Tower hat eine API hinzugefügt, mit der Sie eine Liste der Operationen abrufen können, die kürzlich auf Ihre Landezone angewendet wurden, und der Operationen, die gerade ausgeführt werden. Die API kann den Verlauf der Operationen an der Landezone und deren Identifikatoren für bis zu 90 Tage zurückgeben. Anwendungsbeispiele finden Sie unter Status Ihrer Landezonen-Operationen anzeigen.

Weitere Informationen zur `ListLandingZoneOperations` API finden Sie `ListLandingZoneOperations` in der API-Referenz für AWS Control Tower.

AWS Control Tower unterstützt bis zu 100 gleichzeitige Kontrollvorgänge

20. Mai 2024

(Für die Landezone des AWS Control Tower ist kein Update erforderlich.)

AWS Control Tower unterstützt jetzt mehrere Kontrollvorgänge mit höherer Parallelität. Sie können bis zu 100 AWS Control Tower-Kontrollvorgänge über mehrere Organisationseinheiten (OUs) hinweg

gleichzeitig über die Konsole oder über APIs einreichen. Bis zu zehn (10) Operationen können gleichzeitig ausgeführt werden, und die zusätzlichen werden in die Warteschlange gestellt. Auf diese Weise können Sie eine standardisiertere Konfiguration für mehrere einrichten AWS-Konten, ohne den betrieblichen Aufwand sich wiederholender Kontrollvorgänge hinnehmen zu müssen.

Um den Status Ihrer laufenden und in der Warteschlange befindlichen Kontrollvorgänge zu überwachen, können Sie in der AWS Control Tower-Konsole zur neuen Seite „Letzte Operationen“ navigieren oder die neue `ListControlOperations` API aufrufen.

Die AWS Control Tower-Bibliothek enthält mehr als 500 Kontrollen, die unterschiedlichen Kontrollzielen, Frameworks und Services zugeordnet sind. Für ein bestimmtes Kontrollziel, wie z. B. das Verschlüsseln von Daten im Ruhezustand, können Sie mehrere Steuerelemente mit einem einzigen Kontrollvorgang aktivieren, um das Ziel zu erreichen. Diese Funktion ermöglicht eine beschleunigte Entwicklung, ermöglicht eine schnellere Einführung von Best-Practice-Kontrollen und verringert betriebliche Komplexitäten.

AWS Control Tower ist verfügbar in AWS Kanada West (Calgary)

3. Mai 2024

(Für die Landezone des AWS Control Tower ist kein Update erforderlich.)

Ab heute können Sie den AWS Control Tower in der Region Kanada West (Calgary) aktivieren. Wenn Sie den AWS Control Tower bereits bereitgestellt haben und die Governance-Funktionen auf diese Region ausweiten möchten, können Sie dies mit den AWS Control Tower-APIs für die Landezone tun. Oder gehen Sie von der Konsole aus auf die Seite Einstellungen in Ihrem AWS Control Tower-Dashboard, wählen Sie Ihre Regionen aus und aktualisieren Sie dann Ihre Landing Zone.

Die Region Kanada West (Calgary) unterstützt AWS Service Catalog nicht. Aus diesem Grund unterscheiden sich einige Funktionen von AWS Control Tower. Die bemerkenswerteste Änderung der Funktionalität ist, dass Account Factory nicht verfügbar ist. Wenn Sie Kanada West (Calgary) als Ihre Heimatregion wählen, unterscheiden sich die Verfahren für die Aktualisierung von Konten, die Einrichtung von Kontoautomatisierungen und alle anderen Prozesse, die Service Catalog betreffen, von denen in anderen Regionen.

Bereitstellung von Konten

Um ein neues Konto in der Region Kanada West (Calgary) zu erstellen und bereitzustellen, empfehlen wir Ihnen, ein Konto außerhalb von AWS Control Tower zu erstellen und es dann bei

einer registrierten OU zu registrieren. Weitere Informationen finden Sie unter Ein bestehendes Konto registrieren und Schritte zum Registrieren eines Kontos.

Die Service Catalog-APIs sind in der Region Kanada West (Calgary) nicht verfügbar. Das unter Automatisieren der Kontobereitstellung im AWS Control Tower durch Service Catalog-APIs angezeigte Beispielskript ist nicht funktionsfähig.

Account Factory Customizations (AFC), Account Factory for Terraform (AFT) und Customizations for AWS Control Tower (cFCT) sind in Canada West (Calgary) nicht verfügbar, da es keine anderen zugrunde liegenden Abhängigkeiten für AWS Control Tower gibt. Wenn Sie die Governance auf die Region Kanada West (Calgary) ausdehnen, können Sie weiterhin AFC-Blueprints in allen Regionen verwalten, die AWS Control Tower unterstützt, solange Service Catalog in Ihrer Heimatregion verfügbar ist.

Steuerungen

Proaktive Kontrollen und Kontrollen für den AWS Security Hub CSPM Service-Managed Standard: AWS Control Tower sind in der Region Kanada West (Calgary) nicht verfügbar. Die präventive Steuerung `CT.CLOUDFORMATION.PR.1` ist in Kanada West (Calgary) nicht verfügbar, da sie nur für die Aktivierung der hakenbasierten, proaktiven Kontrollen erforderlich ist. Bestimmte detektivische Kontrollen, die auf basieren, AWS Config sind nicht verfügbar. Details hierzu finden Sie unter Einschränkungen bei der Steuerung.

Identitätsanbieter

IAM Identity Center ist in Canada West (Calgary) nicht verfügbar. Es empfiehlt sich, Ihre Landezone in einer Region einzurichten, in der IAM Identity Center verfügbar ist. Alternativ haben Sie die Möglichkeit, Ihre Kontozugriffskonfiguration selbst zu verwalten, wenn Sie einen externen Identitätsanbieter in Canada West (Calgary) verwenden.

Die Nichtverfügbarkeit von Service Catalog in der Region Kanada West (Calgary) hat keine Auswirkungen auf andere Regionen, die vom AWS Control Tower unterstützt werden. Diese Unterschiede gelten nur, wenn Ihre Heimatregion Kanada West (Calgary) ist.

Eine vollständige Liste der Regionen, in denen AWS Control Tower verfügbar ist, finden Sie AWS in der Regionentabelle.

AWS Control Tower unterstützt Self-Service-Kontingentanpassungen

25. April 2024

(Für die Landezone des AWS Control Tower ist kein Update erforderlich.)

AWS Control Tower unterstützt jetzt Self-Service-Kontingentanpassungen über die Service Quota-Konsole. Weitere Informationen finden Sie unter Anfordern einer Kontingenterhöhung.

AWS Control Tower veröffentlicht den Referenzhandbuch für Steuerungen

21. April 2024

(Für die Landezone des AWS Control Tower ist kein Update erforderlich.)

AWS Control Tower hat den Controls Reference Guide veröffentlicht, ein neues Dokument, in dem Sie detaillierte Informationen zu den Steuerelementen finden, die für die AWS Control Tower-Umgebung spezifisch sind. Zuvor war dieses Material im AWS Control Tower-Benutzerhandbuch enthalten. Das Referenzhandbuch für Steuerelemente behandelt Steuerelemente in einem erweiterten Format. Weitere Informationen finden Sie im Referenzhandbuch für AWS Control Tower Controls.

AWS Control Tower aktualisiert zwei proaktive Kontrollen und benennt sie um

26. März 2024

(Für die Landezone des AWS Control Tower ist kein Update erforderlich.)

AWS Control Tower hat zwei proaktive Steuerungen umbenannt, um sie an die Aktualisierungen von Amazon OpenSearch Service anzupassen.

- [CT.OPENSEARCH.PR.8] Für die Verwendung ist eine Elasticsearch Service-Domain erforderlich TLSv1.2
- [CT.OPENSEARCH.PR.16] Für die Nutzung ist eine Amazon OpenSearch Service-Domain erforderlich TLSv1.2

Wir haben die Kontrollnamen und die Artefakte für diese beiden Steuerelemente aktualisiert, um sie an die aktuelle Version des Amazon OpenSearch Service anzupassen, der jetzt Transport Layer Security (TLS) Version 1.3 als Transportsicherheitsoptionen für die Sicherheit von Domain-Endpunkten unterstützt.

Um Unterstützung TLSv1.3 für diese Steuerelemente hinzuzufügen, haben wir das Artefakt und den Namen der Steuerelemente aktualisiert, um die Absicht der Steuerung widerzuspiegeln. Sie

evaluieren jetzt die TLS-Mindestversion der Servicedomäne. Um dieses Update in Ihrer Umgebung durchzuführen, müssen Sie die Steuerelemente deaktivieren und aktivieren, um das neueste Artefakt bereitzustellen.

Keine anderen proaktiven Steuerungen sind von dieser Änderung betroffen. Wir empfehlen Ihnen, diese Kontrollen zu überprüfen, um sicherzustellen, dass sie Ihren Kontrollzielen entsprechen.

Bei Fragen oder Bedenken wenden Sie sich an den AWS Support.

Veraltete Steuerelemente sind nicht mehr verfügbar

12. März 2024

(Für die Landezone des AWS Control Tower ist kein Update erforderlich.)

Im AWS Control Tower sind einige Steuerelemente veraltet. Diese Steuerelemente sind nicht mehr verfügbar.

- CT.ATHENA.PR.1
- CT.CODEBUILD.PR.4
- CT.AUTOSCALING.PR.3
- SH.Athena.1
- SH.Codebuild.5
- SH.AutoScaling.4
- SH.SNS.1
- SH.SNS.2

AWS Control Tower unterstützt das Taggen von **`EnabledControl`** Ressourcen in CloudFormation

22. Februar 2024

(Für die Landezone des AWS Control Tower ist kein Update erforderlich.)

In dieser Version von AWS Control Tower wird das Verhalten der `EnabledControl` Ressource aktualisiert, um sie besser an die konfigurierbaren Steuerungen anzupassen und die Fähigkeit zu verbessern, Ihre AWS Control Tower-Umgebung mithilfe von Automatisierung zu verwalten. Mit dieser Version können Sie mithilfe von CloudFormation Vorlagen Tags zu konfigurierbaren

`EnabledControl` Ressourcen hinzufügen. Bisher konnten Sie Tags nur über die AWS Control Tower-Konsole und APIs hinzufügen.

Der AWS Control Tower `GetEnabledControl` und die `ListTagsforResource` API-Operationen werden mit dieser Version aktualisiert, da sie auf der `EnabledControl` Ressourcenfunktionalität basieren. `EnableControl`

Weitere Informationen finden Sie unter Tagging von `EnabledControl` Ressourcen im AWS Control Tower und `EnabledControl` im CloudFormation Benutzerhandbuch.

AWS Control Tower unterstützt APIs für die Registrierung und Konfiguration von Organisationseinheiten mit Baselines

14. Februar 2024

(Für die Landezone des AWS Control Tower ist kein Update erforderlich.)

Diese APIs unterstützen die programmatische OU-Registrierung beim `EnableBaseline` Aufruf. Wenn Sie eine Baseline für eine OU aktivieren, werden Mitgliedskonten innerhalb der OU für AWS Control Tower Governance registriert. Es können bestimmte Vorbehalte gelten. Beispielsweise ermöglicht die Registrierung einer Organisationseinheit über die AWS Control Tower-Konsole optionale Kontrollen sowie obligatorische Kontrollen. Wenn Sie APIs aufrufen, müssen Sie möglicherweise einen zusätzlichen Schritt ausführen, damit optionale Steuerelemente aktiviert werden.

Eine AWS Control Tower-Baseline beinhaltet bewährte Methoden für die Verwaltung einer Organisationseinheit und der Mitgliedskonten durch den AWS Control Tower. Wenn Sie beispielsweise eine Baseline für eine OU aktivieren, erhalten Mitgliedskonten innerhalb der OU eine definierte Gruppe von Ressourcen AWS CloudTrail AWS Config, einschließlich IAM Identity Center und der erforderlichen AWS IAM-Rollen.

Bestimmte Baselines sind mit bestimmten Versionen der AWS Control Tower-Landing Zone kompatibel. AWS Control Tower kann die neueste kompatible Basislinie auf Ihre Landezone anwenden, wenn Sie Ihre Landezoneneinstellungen ändern. Weitere Informationen finden Sie unter Kompatibilität von OU-Baselines und landing zone Zone-Versionen.

Diese Version enthält vier wichtige Arten von Basislinien

- `AWSControlTowerBaseline`
- `AuditBaseline`

- `LogArchiveBaseline`
- `IdentityCenterBaseline`

Mit den neuen APIs und definierten Baselines können Sie Organisationseinheiten registrieren und Ihren OU-Bereitstellungsworkflow automatisieren. Die APIs können auch Organisationseinheiten verwalten, die bereits unter der Kontrolle von AWS Control Tower stehen, sodass Sie Organisationseinheiten nach Aktualisierungen der Landezone erneut registrieren können. Die APIs bieten Unterstützung für eine CloudFormation `EnabledBaseline` Ressource, mit der Sie Ihre OUs mit Infrastructure as Code (IaC) verwalten können.

Basis-APIs

- EnableBaseline, UpdateEnabledBaseline, DisableBaseline: Ergreifen Sie Maßnahmen auf der Grundlage einer Organisationseinheit.
- GetEnabledBaseline, ListEnabledBaselines: Entdecken Sie Konfigurationen für Ihre aktivierten Baselines.
- GetBaselineOperation: Zeigen Sie den Status eines bestimmten Basisvorgangs an.
- ResetEnabledBaseline: Beseitigen Sie Ressourcenabweichungen in einer Organisationseinheit mit aktivierter Basislinie (einschließlich verschachtelter Organisationseinheiten und obligatorischer Kontrollabweichungen). Behebt auch die Drift, die durch die Region Deny Control auf Landingzonenebene entsteht
- GetBaseline, ListBaselines: Entdecken Sie den Inhalt der AWS Control Tower-Baselines.

Um mehr über diese APIs zu erfahren, lesen Sie die Baselines im AWS Control Tower-Benutzerhandbuch und in der API-Referenz. https://docs.aws.amazon.com/controltower/latest/APIReference/API_Operations.html Die neuen APIs sind dort verfügbar, AWS-Regionen wo AWS Control Tower verfügbar ist, mit Ausnahme der Regionen GovCloud (USA). Eine Liste der Standorte AWS-Regionen , in denen AWS Control Tower verfügbar ist, finden Sie in der AWS-Region Tabelle.

Januar — Dezember 2023

Im Jahr 2023 veröffentlichte AWS Control Tower die folgenden Updates:

- Übergang zu neuen AWS Service Catalog Externer Produkttyp (Phase 3)
- AWS Control Tower-Landingzone, Version 3.3
- Übergang zu neuen AWS Service Catalog Externer Produkttyp (Phase 2)

- Der AWS Control Tower kündigt Kontrollen zur Unterstützung der digitalen Souveränität an
- APIs für die Landezone von AWS Control Tower
- APIs für das Taggen von AWS Control Tower Control
- AWS Control Tower ist verfügbar in AWS Asien-Pazifik (Melbourne)
- Übergang zu neuen AWS Service Catalog Externer Produkttyp (Phase 1)
- AWS Control Tower fügt eine neue Kontroll-API hinzu
- AWS Control Tower fügt neue Steuerungen hinzu
- AWS Control Tower erkennt vertrauenswürdige Zugriffsabweichungen
- AWS Control Tower ist in vier weiteren Versionen erhältlich AWS-Regionen
- AWS Control Tower verfügbar in AWS Israel (Tel Aviv)
- AWS Control Tower fügt 28 neue proaktive Kontrollen hinzu
- Im AWS Control Tower sind zwei Steuerelemente veraltet
- AWS-Kontrollturm-Landezone, Version 3.2
- AWS Control Tower fügt die Zuordnung von E-Mail zu ID für IAM Identity Center hinzu
- AWS Control Tower fügt weitere hinzu AWS Security Hub CSPM Steuerelemente
- AWS Control Tower veröffentlicht Metadaten für AWS Security Hub CSPM Steuerelemente
- AWS Control Tower fügt Account Factory Customization (AFC) für Terraform hinzu
- AWS Control Tower fügt ein selbstverwaltetes IAM-Identitätscenter hinzu
- AWS Control Tower fügt einen gemischten Hinweis zur Unternehmensführung hinzu
- AWS Control Tower fügt neue proaktive Kontrollen hinzu
- AWS Control Tower aktualisiert die Amazon EC2-Steuerelemente
- AWS Control Tower ist in sieben weiteren erhältlich AWS-Regionen
- AWS Control Tower Account Factory Customization (AFC) und Anforderungsverfolgung sind allgemein verfügbar
- AWS Control Tower-Landezone, Version 3.1
- Proaktive Kontrollen im AWS Control Tower sind allgemein verfügbar

Übergang zu neuen AWS Service Catalog Externer Produkttyp (Phase 3)

14. Dezember 2023

(Für die Landezone des AWS Control Tower ist kein Update erforderlich.)

AWS Control Tower unterstützt Terraform Open Source nicht mehr als Produkttyp (Blueprint) bei der Erstellung neuer Produkte. AWS-Konten Weitere Informationen und Anweisungen zur Aktualisierung Ihrer Konto-Blueprints finden Sie unter Übergang zum AWS Service Catalog externen Produkttyp.

Wenn Sie Ihre Konto-Blueprints nicht aktualisieren, um den Produkttyp Extern zu verwenden, können Sie nur Konten aktualisieren oder kündigen, die Sie mithilfe von Terraform Open Source-Blueprints bereitgestellt haben.

AWS Control Tower-Landingzone, Version 3.3

14. Dezember 2023

(Für die Landing Zone des AWS Control Tower auf Version 3.3 ist ein Update erforderlich. Weitere Informationen finden Sie unterAktualisiere deine landing zone).

Aktualisierungen der S3-Bucket-Richtlinie im AWS Control Tower Audit-Konto

Wir haben die Amazon S3-Audit-Bucket-Richtlinie, die AWS Control Tower in Konten bereitstellt, so geändert, dass eine `aws:SourceOrgID` Bedingung für jegliche Schreibberechtigungen erfüllt sein muss. In dieser Version haben AWS Services nur dann Zugriff auf Ihre Ressourcen, wenn die Anfrage von Ihrer Organisation oder Organisationseinheit (OU) stammt.

Sie können den `aws:SourceOrgID` Bedingungsschlüssel verwenden und den Wert auf Ihre Organisations-ID im Bedingungselement Ihrer S3-Bucket-Richtlinie setzen. Diese Bedingung stellt sicher, dass CloudTrail nur Protokolle im Namen von Konten innerhalb Ihrer Organisation in Ihren S3-Bucket geschrieben werden können; sie verhindert, dass CloudTrail Protokolle außerhalb Ihrer Organisation in Ihren AWS Control Tower S3-Bucket schreiben.

Wir haben diese Änderung vorgenommen, um eine potenzielle Sicherheitslücke zu beheben, ohne die Funktionalität Ihrer vorhandenen Workloads zu beeinträchtigen. Die aktualisierte Richtlinie finden Sie unter. Amazon S3 S3-Bucket-Richtlinie für die Protokollierung

Weitere Informationen zum neuen Bedingungsschlüssel finden Sie in der IAM-Dokumentation und im IAM-Blogbeitrag mit dem Titel „Verwenden Sie skalierbare Steuerelemente für AWS Dienste, die auf Ihre Ressourcen zugreifen“.

Aktualisierungen der Richtlinie im SNS-Thema AWS Config

Wir haben den neuen `aws:SourceOrgID` Bedingungsschlüssel zur Richtlinie für das AWS Config SNS-Thema hinzugefügt. Informationen zur aktualisierten Richtlinie finden Sie unter Die AWS Config SNS-Themenrichtlinie.

Aktualisierungen der Landezone Region Deny Control

- `discovery-marketplace:` wurde entfernt. Diese Maßnahme fällt unter die `aws-marketplace:*` Ausnahmeregelung.
- `quicksight:DescribeAccountSubscription` hinzugefügt

CloudFormation Vorlage wurde aktualisiert

Wir haben die CloudFormation Vorlage für den benannten Stack aktualisiert, `BASELINE-CLOUDTRAIL-MASTER` sodass keine Abweichungen auftreten, wenn keine AWS KMS Verschlüsselung verwendet wird.

Übergang zu neuen AWS Service Catalog Externer Produkttyp (Phase 2)

7. Dezember 2023

(Für die Landezone des AWS Control Tower ist kein Update erforderlich.)

HashiCorp hat ihre Terraform-Lizenzierung aktualisiert. Infolgedessen wurde die Unterstützung für Terraform Open Source-Produkte und bereitgestellte Produkte auf einen neuen Produkttyp namens External AWS Service Catalog umgestellt.

Um eine Unterbrechung der vorhandenen Workloads und AWS Ressourcen in Ihren Konten zu vermeiden, befolgen Sie bis zum 14. Dezember 2023 die Schritte zur Umstellung auf den AWS Control Tower unter Umstellung auf den Produkttyp „ AWS Service Catalog Extern“.

Der AWS Control Tower kündigt Kontrollen zur Unterstützung der digitalen Souveränität an

27. November 2023

(Für die Landezone des AWS Control Tower ist kein Update erforderlich.)

AWS Control Tower kündigt 65 neue AWS verwaltete Steuerungen an, mit denen Sie Ihre Anforderungen an die digitale Souveränität erfüllen können. In dieser Version können Sie diese Kontrollen unter einer neuen Gruppe für digitale Souveränität in der AWS Control Tower-Konsole entdecken. Mithilfe dieser Steuerelemente können Sie Aktionen verhindern und Ressourcenänderungen in Bezug auf Datenspeicherort, granulare Zugriffsbeschränkungen , Verschlüsselung und Resilienzfunktionen erkennen. Diese Steuerelemente sollen es Ihnen erleichtern, Anforderungen in großem Umfang zu erfüllen. Weitere Informationen zu Kontrollen der

digitalen Souveränität finden Sie unter Kontrollen zur Verbesserung des Schutzes der digitalen Souveränität.

Sie können beispielsweise Steuerelemente aktivieren, mit denen Sie Ihre Verschlüsselungs- und Resilienzstrategien durchsetzen können, wie z. B. Erfordern Sie einen AWS AppSync API-Cache, um die Verschlüsselung während der Übertragung zu aktivieren, oder Erfordern Sie, dass eine AWS Netzwerk-Firewall über mehrere Availability Zones verteilt ist. Sie können die Ablehnungskontrolle für die Region im AWS Control Tower auch so anpassen, dass regionale Einschränkungen gelten, die Ihren individuellen Geschäftsanforderungen am besten entsprechen.

Diese Version bietet deutlich erweiterte Funktionen zum Ablehnen von Regionen im AWS Control Tower. Sie können eine neue, parametrisierte Region-Deny-Control auf OU-Ebene anwenden, um die Granularität der Steuerung zu erhöhen und gleichzeitig eine zusätzliche Region-Governance auf der Landing-Zone-Ebene beizubehalten. Diese anpassbare Steuerung zur Verweigerung von Regionen hilft Ihnen dabei, regionale Einschränkungen anzuwenden, die Ihren individuellen Geschäftsanforderungen am besten entsprechen. Weitere Informationen zur neuen, konfigurierbaren Regionsverweigerungskontrolle finden Sie unter Auf die Organisationseinheit angewendete Regionsverweigerungskontrolle.

Als neues Tool für die neue Erweiterung „Region Deny“ enthält diese Version eine neue API`UpdateEnabledControl`, mit der Sie Ihre aktivierten Steuerelemente auf die Standardeinstellungen zurücksetzen können. Diese API ist besonders hilfreich in Anwendungsfällen, in denen Sie Abweichungen schnell beheben oder programmgesteuert sicherstellen müssen, dass sich ein Steuerelement nicht im Drift-Zustand befindet. Weitere Informationen zur neuen API finden Sie in der AWS Control Tower API-Referenz

Neue proaktive Kontrollen

- CT.APIGATEWAY.PR.6: Erfordern Sie, dass eine Amazon API Gateway-REST-Domain eine Sicherheitsrichtlinie verwendet, die eine Mindestversion des TLS-Protokolls von festlegt TLSv1.2
- CT.APPSYNC.PR.2: Erfordert, dass eine AWS AppSync GraphQL-API mit privater Sichtbarkeit konfiguriert wird
- CT.APPSYNC.PR.3: Erfordert, dass eine AWS AppSync GraphQL-API nicht mit API-Schlüsseln authentifiziert wird
- CT.APPSYNC.PR.4: Erfordert einen AWS AppSync GraphQL-API-Cache, um die Verschlüsselung bei der Übertragung zu aktivieren.
- CT.APPSYNC.PR.5: Erfordert einen AWS AppSync GraphQL-API-Cache, um die Verschlüsselung im Ruhezustand zu aktivieren.

- CT.AUTOSCALING.PR.9: Erfordert ein Amazon EBS-Volume, das über eine Amazon EC2 Auto Scaling-Startkonfiguration konfiguriert wurde, um Daten im Ruhezustand zu verschlüsseln
- CT.AUTOSCALING.PR.10: Erfordern Sie, dass eine Amazon EC2 Auto Scaling-Gruppe beim Überschreiben einer Startvorlage nur AWS Nitro-Instance-Typen verwendet
- CT.AUTOSCALING.PR.11: Erfordert, dass nur AWS Nitro-Instance-Typen, die die Verschlüsselung des Netzwerkverkehrs zwischen Instances unterstützen, einer Amazon EC2 Auto Scaling-Gruppe hinzugefügt werden, wenn eine Startvorlage überschrieben wird
- CT.DAX.PR.3: Erfordert einen DynamoDB Accelerator-Cluster, um Daten bei der Übertragung mit Transport Layer Security (TLS) zu verschlüsseln
- CT.DMS.PR.2: Erfordert einen DMS-Endpunkt (AWS Database Migration Service), um Verbindungen für Quell- und Zielendpunkte zu verschlüsseln
- CT.EC2.PR.15: Erfordert, dass eine Amazon EC2-Instance beim Erstellen anhand des Ressourcentyps einen AWS Nitro-Instance-Typ verwendet `AWS::EC2::LaunchTemplate`
- CT.EC2.PR.16: Erfordert, dass eine Amazon EC2-Instance einen AWS Nitro-Instance-Typ verwendet, wenn sie mit dem Ressourcentyp erstellt wird `AWS::EC2::Instance`
- CT.EC2.PR.17: Erfordert einen dedizierten Amazon EC2-Host, um einen AWS Nitro-Instance-Typ zu verwenden
- CT.EC2.PR.18: Erfordern Sie, dass eine Amazon EC2-Flotte nur die Startvorlagen mit AWS Nitro-Instance-Typen außer Kraft setzt
- CT.EC2.PR.19: Erfordert, dass eine Amazon EC2-Instance einen Nitro-Instance-Typ verwendet, der Verschlüsselung bei der Übertragung zwischen Instances unterstützt, wenn sie mit dem Ressourcentyp erstellt wird `AWS::EC2::Instance`
- CT.EC2.PR.20: Erfordern Sie, dass eine Amazon EC2-Flotte nur die Startvorlagen mit AWS Nitro-Instance-Typen überschreibt, die die Verschlüsselung bei der Übertragung zwischen Instances unterstützen
- CT.ELASTICACHE.PR.8: Erfordert eine ElastiCache Amazon-Replikationsgruppe späterer Redis-Versionen, um die RBAC-Authentifizierung zu aktivieren
- CT.MQ.PR.1: Erfordern Sie, dass ein Amazon MQ ActiveMQ-Broker den Bereitstellungsmodus für hohe Verfügbarkeit verwendet active/standby
- CT.MQ.PR.2: Erfordern Sie, dass ein Amazon MQ Rabbit MQ-Broker den Cluster-Modus für Hochverfügbarkeit verwendet Multi-AZ
- CT.MSK.PR.1: Erfordern Sie einen Amazon Managed Streaming for Apache Kafka (MSK) -Cluster, um die Verschlüsselung bei der Übertragung zwischen Cluster-Broker-Knoten durchzusetzen

- CT.MSK.PR.2: Erfordert, dass ein Amazon Managed Streaming for Apache Kafka (MSK) -Cluster deaktiviert konfiguriert ist PublicAccess
- CT.NETWORK-FIREWALL.PR.5: Erfordert die Bereitstellung einer AWS Netzwerk-Firewall-Firewall in mehreren Availability Zones
- CT.RDS.PR.26: Erfordern Sie einen Amazon RDS DB-Proxy, um Transport Layer Security (TLS) -Verbindungen zu benötigen
- CT.RDS.PR.27: Erfordern Sie eine Amazon RDS-DB-Cluster-Parametergruppe, um Transport Layer Security (TLS) -Verbindungen für unterstützte Engine-Typen zu benötigen
- CT.RDS.PR.28: Erfordert eine Amazon RDS-DB-Parametergruppe, um Transport Layer Security (TLS) -Verbindungen für unterstützte Engine-Typen zu benötigen
- CT.RDS.PR.29: Erfordert, dass ein Amazon RDS-Cluster nicht so konfiguriert ist, dass er über die Eigenschaft 'PubliclyAccessible' öffentlich zugänglich ist
- CT.RDS.PR.30: Erfordert, dass für eine Amazon RDS-Datenbank-Instance die Verschlüsselung im Ruhezustand so konfiguriert ist, dass sie einen KMS-Schlüssel verwendet, den Sie für unterstützte Engine-Typen angeben
- CT.S3.PR.12: Erfordern Sie, dass ein Amazon S3-Zugangspunkt über eine BPA-Konfiguration (Block Public Access) verfügt, bei der alle Optionen auf „true“ gesetzt sind

Neue präventive Kontrollen

- CT.APPSYNC.PV.1Erfordern Sie, dass eine AWS AppSync GraphQL-API mit privater Sichtbarkeit konfiguriert ist
- CT.EC2.PV.1Erfordern Sie, dass ein Amazon EBS-Snapshot aus einem verschlüsselten EC2-Volume erstellt wird
- CT.EC2.PV.2Erfordern Sie, dass ein angehängtes Amazon EBS-Volume so konfiguriert ist, dass ruhende Daten verschlüsselt werden
- CT.EC2.PV.3Erfordern Sie, dass ein Amazon EBS-Snapshot nicht öffentlich wiederherstellbar ist
- CT.EC2.PV.4Erfordern Sie, dass die direkten Amazon EBS-APIs nicht aufgerufen werden
- CT.EC2.PV.5Verbieten Sie die Verwendung des Imports und Exports von Amazon EC2-VMs
- CT.EC2.PV.6Verbieten Sie die Verwendung veralteter Amazon EC2- und API-Aktionen RequestSpotFleet RequestSpotInstances
- CT.KMS.PV.1Eine AWS KMS wichtige Richtlinie muss eine Erklärung enthalten, die die Gewährung von Zuschüssen auf Dienstleistungen beschränkt AWS KMS AWS

- CT.KMS.PV.2Erfordern Sie, dass ein AWS KMS asymmetrischer Schlüssel mit RSA-Schlüsselmaterial, das für die Verschlüsselung verwendet wird, keine Schlüssellänge von 2048 Bit hat
- CT.KMS.PV.3Erfordern Sie, dass bei der Konfiguration eines AWS KMS Schlüssels die Sicherheitsüberprüfung für die Sperrung der Umgehungsrichtlinie aktiviert ist
- CT.KMS.PV.4Erfordern Sie, dass ein AWS KMS vom Kunden verwalteter Schlüssel (CMK) mit Schlüsselmaterial konfiguriert ist, das von CloudHSM stammt AWS
- CT.KMS.PV.5Erfordern Sie, dass ein AWS KMS vom Kunden verwalteter Schlüssel (CMK) mit importiertem Schlüsselmaterial konfiguriert wird
- CT.KMS.PV.6Erfordern Sie, dass AWS KMS ein vom Kunden verwalteter Schlüssel (CMK) mit Schlüsselmaterial konfiguriert wird, das aus einem externen Schlüsselspeicher (XKS) stammt
- CT.LAMBDA.PV.1Für die Authentifizierung ist eine AWS Lambda Funktions-URL erforderlich AWS IAM-based
- CT.LAMBDA.PV.2Erfordern Sie, dass eine AWS Lambda Funktions-URL so konfiguriert ist, dass nur Prinzipale in Ihrem AWS-Konto

APIs für die Landezone von AWS Control Tower

26. November 2023

(Für die Landungszone des AWS Control Tower ist kein Update erforderlich.)

AWS Control Tower bietet jetzt APIs, mit denen Sie Ihre Landezone programmgesteuert verwalten können. Mit diesen APIs können Sie Ihre Landezone erstellen, aktualisieren und zurücksetzen sowie Informationen über die Konfiguration und den Betrieb Ihrer Landezone abrufen. Weitere Informationen finden Sie unter Beispiele für Landingzone-APIs.

Die Landing Zone-APIs sind in allen Regionen verfügbar, in AWS-Regionen denen AWS Control Tower verfügbar ist, mit Ausnahme der Regionen GovCloud (USA). Eine Liste der Standorte AWS-Regionen , in denen AWS Control Tower verfügbar ist, finden Sie in der AWS-Region Tabelle.

APIs für das Taggen von AWS Control Tower Control

10. November 2023

(Für die AWS Control Tower-Landezone ist kein Update erforderlich.)

AWS Control Tower bietet jetzt APIs, mit denen Sie Ihre aktivierten Steuerelemente programmgesteuert taggen können. Mit diesen APIs können Sie Tags für Ihre aktivierten Steuerelemente hinzufügen, entfernen und auflisten. Weitere Informationen finden Sie unter Tagging von AWS Control Tower-Ressourcen.

Die Control-Tagging-APIs sind in allen Regionen verfügbar, in AWS-Regionen denen AWS Control Tower verfügbar ist, mit Ausnahme der Regionen GovCloud (USA). Eine Liste der Standorte AWS-Regionen , in denen AWS Control Tower verfügbar ist, finden Sie in der AWS-Region Tabelle.

AWS Control Tower ist verfügbar in AWS Asien-Pazifik (Melbourne)

3. November 2023

(Für die AWS Control Tower-Landezone ist kein Update erforderlich.)

AWS Control Tower ist im asiatisch-pazifischen Raum (Melbourne) verfügbar. Eine vollständige Liste der Regionen, in denen AWS Control Tower verfügbar ist, finden Sie in der AWS-Region Tabelle.

Übergang zu neuen AWS Service Catalog Externer Produkttyp (Phase 1)

31. Oktober 2023

(Für die AWS Control Tower-Landezone ist kein Update erforderlich.)

HashiCorp hat ihre Terraform-Lizenzierung aktualisiert. Infolgedessen wurde die Unterstützung für Terraform Open Source-Produkte und bereitgestellte Produkte auf einen neuen Produkttyp namens External AWS Service Catalog umgestellt.

Um eine Unterbrechung der vorhandenen Workloads und AWS Ressourcen in Ihren Konten zu vermeiden, befolgen Sie bis zum 14. Dezember 2023 die Schritte zur Umstellung auf den AWS Control Tower unter Umstellung auf den Produkttyp „ AWS Service Catalog Extern“.

AWS Control Tower fügt eine neue Kontroll-API hinzu

27. Oktober 2023

(Für die AWS Control Tower-Landezone ist kein Update erforderlich.)

AWS Control Tower bietet jetzt eine neue API`UpdateEnabledControl`, mit der Sie Ihre aktivierten Steuerelemente aktualisieren können. Diese API ist besonders hilfreich in Anwendungsfällen, in denen Sie Abweichungen schnell beheben oder programmgesteuert sicherstellen müssen, dass sich

eine Steuerung nicht im Drift-Zustand befindet. Weitere Informationen zur neuen API finden Sie in der AWS Control Tower API-Referenz.

Die `UpdateEnabledControl` API ist in allen Regionen verfügbar, in AWS-Regionen denen AWS Control Tower verfügbar ist, mit Ausnahme der Regionen GovCloud (USA). Eine Liste der Standorte AWS-Regionen , in denen AWS Control Tower verfügbar ist, finden Sie in der AWS-Region Tabelle.

AWS Control Tower fügt neue Steuerungen hinzu

20. Oktober 2023

(Für die AWS Control Tower-Landezone ist kein Update erforderlich.)

AWS Control Tower hat der Steuerelementbibliothek von AWS Control Tower 22 neue Steuerelemente hinzugefügt. Diese Kontrollen helfen Ihnen dabei, bewährte Methoden für Ihre AWS Ressourcen durchzusetzen. Weitere Informationen zu den neuen Kontrollen finden Sie unter Kontrollkategorien.

Die neuen Steuerelemente sind überall dort verfügbar AWS-Regionen , wo AWS Control Tower verfügbar ist. Eine Liste der Standorte AWS-Regionen , an denen AWS Control Tower verfügbar ist, finden Sie in der AWS-Region Tabelle.

AWS Control Tower erkennt vertrauenswürdige Zugriffsabweichungen

13. Oktober 2023

(Für die AWS Control Tower-Landezone ist kein Update erforderlich.)

Der AWS Control Tower erkennt jetzt Abweichungen bei den vertrauenswürdigen Zugriffseinstellungen und meldet sie. Vertrauenswürdige Zugriffseinstellungen ermöglichen es AWS Control Tower, in Ihrem Namen mit anderen AWS Diensten zu interagieren. Wenn diese Einstellungen außerhalb von AWS Control Tower geändert werden, erkennt AWS Control Tower die Abweichung und meldet sie in der AWS Control Tower-Konsole. Weitere Informationen zu Trusted Access Drift finden Sie unter Arten der Governance-Drift.

Die Erkennung vertrauenswürdiger Zugriffsabweichungen ist überall dort verfügbar AWS-Regionen , wo der AWS Control Tower verfügbar ist. Eine Liste der Standorte AWS-Regionen , an denen AWS Control Tower verfügbar ist, finden Sie in der AWS-Region Tabelle.

AWS Control Tower ist in vier weiteren Versionen erhältlich AWS-Regionen

29. September 2023

(Für die AWS Control Tower-Landezone ist kein Update erforderlich.)

AWS Control Tower ist in vier weiteren Ländern verfügbar AWS-Regionen: Asien-Pazifik (Hyderabad), Asien-Pazifik (Jakarta), Europa (Spanien) und Europa (Zürich). Eine vollständige Liste der Regionen, in denen AWS Control Tower verfügbar ist, finden Sie in der AWS-Region Tabelle.

AWS Control Tower verfügbar in AWS Israel (Tel Aviv)

1. August 2023

(Für die AWS Control Tower-Landezone ist kein Update erforderlich.)

Der AWS Control Tower ist in Israel (Tel Aviv) verfügbar. Eine vollständige Liste der Regionen, in denen der AWS Control Tower verfügbar ist, finden Sie in der AWS-Region Tabelle.

AWS Control Tower fügt 28 neue proaktive Kontrollen hinzu

27. Juli 2023

(Für die AWS Control Tower-Landezone ist kein Update erforderlich.)

AWS Control Tower hat der Kontrollbibliothek von AWS Control Tower 28 neue proaktive Kontrollen hinzugefügt. Diese Kontrollen helfen Ihnen dabei, bewährte Verfahren für Ihre AWS Ressourcen durchzusetzen. Weitere Informationen zu den neuen Kontrollen finden Sie unter Kontrollkategorien.

Die neuen Steuerelemente sind überall dort verfügbar AWS-Regionen , wo AWS Control Tower verfügbar ist. Eine Liste der Standorte AWS-Regionen , an denen AWS Control Tower verfügbar ist, finden Sie in der AWS-Region Tabelle.

Im AWS Control Tower sind zwei Steuerelemente veraltet

27. Juli 2023

(Für die AWS Control Tower-Landezone ist kein Update erforderlich.)

Im AWS Control Tower sind zwei Steuerelemente veraltet: CT.CLOUDFORMATION.PR.2 und. CT.CLOUDFORMATION.PR.3 Diese Steuerelemente sind in der Kontrollbibliothek von AWS Control Tower nicht mehr verfügbar. Weitere Informationen zu den veralteten Steuerelementen finden Sie unter Kontrollkategorien.

Die veralteten Steuerelemente sind in keinem mehr verfügbar. AWS-Region

AWS-Kontrollturm-Landezone, Version 3.2

16. Juni 2023

(Für die AWS Control Tower-Landezone auf Version 3.2 ist ein Update erforderlich. Weitere Informationen finden Sie unterAktualisiere deine landing zone).

Mit der Version 3.2 der AWS Control Tower Landing Zone sind die Steuerungen, die Teil des AWS Security Hub CSPM Service-Managed Standards sind: AWS Control Tower, allgemein verfügbar. Es bietet die Möglichkeit, den Drift-Status von Steuerungen, die Teil dieses Standards sind, in der AWS Control Tower-Konsole einzusehen.

Dieses Update beinhaltet eine neue Service-Linked Role (SLR) namens. AWSServiceRoleForAWSControlTower Diese Rolle unterstützt AWS Control Tower bei der Erstellung einer EventBridge verwalteten Regel, die AWSControlTowerManagedRule in jedem Mitgliedskonto als „" bezeichnet wird“. Diese verwaltete Regel erfasst AWS Security Hub CSPM Finding-Ereignisse, anhand derer mithilfe des AWS Control Tower Kontrollabweichungen ermittelt werden können.

Diese Regel ist die erste verwaltete Regel, die von AWS Control Tower erstellt wird. Die Regel wird nicht von einem Stack bereitgestellt; sie wird direkt über die EventBridge APIs bereitgestellt. Sie können die Regel in der EventBridge Konsole oder mithilfe der EventBridge APIs anzeigen. Wenn das `managed-by` Feld ausgefüllt ist, wird der AWS Control Tower-Serviceprinzipal angezeigt.

Zuvor hatte AWS Control Tower die AWSControlTowerExecution Aufgabe übernommen, Operationen in Mitgliedskonten durchzuführen. Diese neue Rolle und Regel entsprechen besser dem bewährten Prinzip, bei der Ausführung von Vorgängen in einer AWS Umgebung mit mehreren Konten die geringsten Rechte zu gewähren. Die neue Rolle bietet erweiterte Berechtigungen, die insbesondere Folgendes ermöglichen: die Erstellung der verwalteten Regel in Mitgliedskonten, die Verwaltung der verwalteten Regel, die Veröffentlichung von Sicherheitsbenachrichtigungen über SNS und die Überprüfung von Abweichungen. Weitere Informationen finden Sie unter AWSServiceRoleForAWSControlTower.

Das Landing Zone 3.2-Update beinhaltet auch eine neue StackSet Ressource im VerwaltungskontoBP_BASELINE_SERVICE_LINKED_ROLE, das zunächst die serviceverknüpfte Rolle bereitstellt.

Wenn der Security Hub CSPM eine Drift bei der Steuerung meldet (in der Landezone 3.2 und höher), erhält der AWS Control Tower täglich ein Status-Update von Security Hub CSPM. Obwohl

die Kontrollen in jeder regulierten Region aktiv sind, sendet der AWS Control Tower die AWS Security Hub CSPM Finding-Ereignisse nur an die Heimatregion des AWS Control Tower. Weitere Informationen finden Sie unter Security Hub — Berichte über Kontrollabweichungen.

Aktualisieren Sie die Kontrolle über die Region: Verweigern

Diese Version der Landezone beinhaltet auch ein Update für das Steuerelement Region Deny.

Globale Dienste und APIs hinzugefügt

- AWS Fakturierung und Kostenmanagement (`billing:*`)
- AWS CloudTrail (`cloudtrail:LookupEvents`), um die Sichtbarkeit globaler Ereignisse in den Mitgliedskonten zu ermöglichen.
- AWS Konsolidierte Fakturierung (`consolidatedbilling:*`)
- AWS Mobile Anwendung für die Managementkonsole (`consoleapp:*`)
- AWS Kostenloses Kontingent (`freetier:*`)
- AWS Invoicing (`invoicing:*`)
- AWS IQ (`iq:*`)
- AWS Benutzerbenachrichtigungen (`notifications:*`)
- AWS Benutzerbenachrichtigungen Kontakte (`notifications-contacts:*`)
- Amazon Payments (`payments:*`)
- AWS Steuereinstellungen (`tax:*`)

Globale Dienste und APIs wurden entfernt

- Wurde entfernt`s3:GetAccountPublic`, da es sich nicht um eine gültige Aktion handelt.
- Wurde entfernt`s3:PutAccountPublic`, weil es sich nicht um eine gültige Aktion handelt.

AWS Control Tower fügt die Zuordnung von E-Mail zu ID für IAM Identity Center hinzu

13. Juli 2023

(Für die AWS Control Tower-Landezone ist kein Update erforderlich.)

AWS Control Tower unterstützt jetzt die Zuordnung von E-Mail zu ID für IAM Identity Center. Mit dieser Funktion können Sie E-Mail-Adressen IAM Identity Center-Benutzer-IDs zuordnen, was die Verwaltung des Benutzerzugriffs auf Ihre AWS Control Tower-Umgebung erleichtert. Weitere Informationen zur Zuordnung von E-Mails zu IDs finden Sie unter Integration mit IAM Identity Center.

Email-to-ID Mapping ist überall dort verfügbar AWS-Regionen , wo AWS Control Tower verfügbar ist. Eine Liste der Standorte AWS-Regionen , an denen AWS Control Tower verfügbar ist, finden Sie in der AWS-Region Tabelle.

AWS Control Tower fügt weitere hinzu AWS Security Hub CSPM Steuerelemente

29. Juni 2023

(Für die AWS Control Tower-Landezone ist kein Update erforderlich.)

AWS Control Tower hat der AWS Security Hub CSPM Steuerelementbibliothek von AWS Control Tower weitere Steuerelemente hinzugefügt. Diese Kontrollen helfen Ihnen dabei, bewährte Methoden für Ihre AWS Ressourcen durchzusetzen. Weitere Informationen zu den neuen Kontrollen finden Sie unter Kontrollkategorien.

Die neuen Steuerelemente sind überall dort verfügbar AWS-Regionen , wo AWS Control Tower verfügbar ist. Eine Liste der Standorte AWS-Regionen , an denen AWS Control Tower verfügbar ist, finden Sie in der AWS-Region Tabelle.

AWS Control Tower veröffentlicht Metadaten für AWS Security Hub CSPM Steuerelemente

22. Juni 2023

(Für die AWS Control Tower-Landezone ist kein Update erforderlich.)

AWS Control Tower veröffentlicht jetzt Metadaten für AWS Security Hub CSPM Kontrollen. Diese Metadaten enthalten Informationen über die Kontrolle, wie z. B. die Kontroll-ID, den Kontrolltitel und die Kontrollbeschreibung. Weitere Informationen zu den Metadaten finden Sie unter Steuerelement-Metadaten.

Kontrollmetadaten sind überall dort verfügbar AWS-Regionen , wo AWS Control Tower verfügbar ist. Eine Liste der Standorte AWS-Regionen , an denen AWS Control Tower verfügbar ist, finden Sie in der AWS-Region Tabelle.

AWS Control Tower fügt Account Factory Customization (AFC) für Terraform hinzu

15. Juni 2023

(Für die AWS Control Tower-Landezone ist kein Update erforderlich.)

AWS Control Tower unterstützt jetzt Account Factory Customization (AFC) für Terraform. Mit dieser Funktion können Sie Terraform verwenden, um Ihre AWS Control Tower-Konten anzupassen. Weitere Informationen zu AFC für Terraform finden Sie unter Account Factory-Anpassung für Terraform.

AFC for Terraform ist überall dort verfügbar, wo AWS Control Tower verfügbar ist. AWS-Regionen Eine Liste der Standorte, an AWS-Regionen denen AWS Control Tower verfügbar ist, finden Sie in der Tabelle. AWS-Region

AWS Control Tower fügt ein selbstverwaltetes IAM-Identitätscenter hinzu

8. Juni 2023

(Für die AWS Control Tower-Landezone ist kein Update erforderlich.)

AWS Control Tower unterstützt jetzt das selbstverwaltete IAM-Identitätscenter. Mit dieser Funktion können Sie Ihren eigenen Identitätsanbieter mit AWS Control Tower verwenden. Weitere Informationen zum selbstverwalteten IAM-Identitätscenter finden Sie unter IAM-Identitätscenter.

Self-managed Das IAM Identity Center ist überall dort verfügbar, AWS-Regionen wo der AWS Control Tower verfügbar ist. Eine Liste der Standorte AWS-Regionen , an denen AWS Control Tower verfügbar ist, finden Sie in der AWS-Region Tabelle.

AWS Control Tower fügt einen gemischten Hinweis zur Unternehmensführung hinzu

1. Juni 2023

(Für die AWS Control Tower-Landezone ist kein Update erforderlich.)

Der AWS Control Tower enthält jetzt einen Hinweis zur gemischten Verwaltung. In diesem Hinweis wird erläutert, wie AWS Control Tower mit anderen AWS Diensten zusammenarbeitet, um die Verwaltung Ihrer AWS Ressourcen zu gewährleisten. Weitere Informationen zur gemischten Unternehmensführung finden Sie unter Mixed Governance.

Die Mixed Governance Note ist überall dort verfügbar AWS-Regionen , wo AWS Control Tower verfügbar ist. Eine Liste der Standorte AWS-Regionen , an denen AWS Control Tower verfügbar ist, finden Sie in der AWS-Region Tabelle.

AWS Control Tower fügt neue proaktive Kontrollen hinzu

25. Mai 2023

(Für die AWS Control Tower-Landezone ist kein Update erforderlich.)

AWS Control Tower hat der Kontrollbibliothek von AWS Control Tower neue proaktive Kontrollen hinzugefügt. Diese Kontrollen helfen Ihnen dabei, bewährte Verfahren für Ihre AWS Ressourcen durchzusetzen. Weitere Informationen zu den neuen Kontrollen finden Sie unter Kontrollkategorien.

Die neuen Steuerelemente sind überall dort verfügbar AWS-Regionen , wo AWS Control Tower verfügbar ist. Eine Liste der Standorte AWS-Regionen , an denen AWS Control Tower verfügbar ist, finden Sie in der AWS-Region Tabelle.

AWS Control Tower aktualisiert die Amazon EC2-Steuerelemente

18. Mai 2023

(Für die AWS Control Tower-Landezone ist kein Update erforderlich.)

AWS Control Tower hat die Amazon EC2-Steuerelemente in der Steuerelementbibliothek von AWS Control Tower aktualisiert. Diese Updates verbessern die Sicherheit und Zuverlässigkeit Ihrer AWS Control Tower-Umgebung. Weitere Informationen zu den aktualisierten Steuerelementen finden Sie unter Kontrollkategorien.

Die aktualisierten Steuerelemente sind überall dort verfügbar AWS-Regionen , wo AWS Control Tower verfügbar ist. Eine Liste der Standorte AWS-Regionen , an denen AWS Control Tower verfügbar ist, finden Sie in der AWS-Region Tabelle.

AWS Control Tower ist in sieben weiteren erhältlich AWS-Regionen

11. Mai 2023

(Für die AWS Control Tower-Landezone ist kein Update erforderlich.)

AWS Control Tower ist in sieben weiteren Ländern verfügbar AWS-Regionen: Asien-Pazifik (Osaka), Kanada (Zentral), Europa (Mailand), Europa (Stockholm), Naher Osten (Bahrain), Naher Osten (VAE)

und Südamerika (São Paulo). Eine vollständige Liste der Regionen, in denen AWS Control Tower verfügbar ist, finden Sie in der AWS-Region Tabelle.

AWS Control Tower Account Factory Customization (AFC) und Anforderungsverfolgung sind allgemein verfügbar

27. April 2023

(Für die AWS Control Tower-Landezone ist kein Update erforderlich.)

AWS Control Tower Account Factory Customization (AFC) und Anforderungsverfolgung sind jetzt allgemein verfügbar. Mit AFC können Sie Ihre AWS Control Tower-Konten anpassen, und mithilfe der Anforderungsverfolgung können Sie den Status Ihrer AWS Control Tower-Anfragen verfolgen. Weitere Informationen zu AFC und Anforderungsverfolgung finden Sie unter Account Factory-Anpassung und Anforderungsverfolgung. https://docs.aws.amazon.com/controltower/latest/userguide/request-tracing.html

AFC und Anforderungsverfolgung sind überall dort verfügbar, AWS-Regionen wo AWS Control Tower verfügbar ist. Eine Liste der Standorte AWS-Regionen , an denen AWS Control Tower verfügbar ist, finden Sie in der AWS-Region Tabelle.

AWS Control Tower-Landezone, Version 3.1

9. Februar 2023

(Für die AWS Control Tower-Landezone auf Version 3.1 ist ein Update erforderlich. Weitere Informationen finden Sie unterAktualisiere deine landing zone)

Die Version 3.1 der AWS Control Tower-Landing Zone umfasst die folgenden Updates:

- Mit dieser Version deaktiviert AWS Control Tower die unnötige Zugriffsprotokollierung für Ihren Access Logging Bucket. Dabei handelt es sich um den Amazon S3-Bucket, in dem Zugriffsprotokolle im Log Archive-Konto gespeichert werden, und aktiviert gleichzeitig weiterhin die Serverzugriffsprotokollierung für S3-Buckets. Diese Version enthält auch Aktualisierungen der Steuerung „Region verweigern“, die zusätzliche Aktionen für globale Dienste wie Support Pläne und ermöglichen. AWS Artifact
- Die Deaktivierung der Serverzugriffsprotokollierung für den AWS Control Tower Access Logging Bucket veranlasst Security Hub CSPM, ein Ergebnis für den Zugriffsprotokollierungs-Bucket des Log Archive-Kontos zu erstellen. Aufgrund einer AWS Security Hub CSPM Regel sollte die [S3.9] S3-Bucket-Serverzugriffsprotokollierung aktiviert sein. In Übereinstimmung mit Security Hub

CSPM empfehlen wir, dieses spezielle Ergebnis zu unterdrücken, wie in der Security Hub CSPM-Beschreibung dieser Regel angegeben. Weitere Informationen finden Sie unter Informationen zu unterdrückten Ergebnissen.

- Die Zugriffsprotokollierung für den (regulären) Logging-Bucket im Log Archive-Konto ist in Version 3.1 unverändert. Gemäß den bewährten Methoden werden Zugriffsereignisse für diesen Bucket als Logeinträge im Access Logging Bucket aufgezeichnet. Weitere Informationen zur Zugriffsprotokollierung finden Sie unter Protokollieren von Anfragen mithilfe der Serverzugriffsprotokollierung in der Amazon S3-Dokumentation.
- Wir haben die Steuerung Region Deny aktualisiert. Dieses Update ermöglicht Aktionen von mehr globalen Diensten. Einzelheiten zu diesem SCP finden Sie unter Zugriff auf AWS basierend auf den angeforderten Einstellungen verweigern AWS-Region und unter Kontrollen, die den Schutz der Datenresidenz verbessern.

  Globale Dienste haben hinzugefügt:

  - AWS -Kontenverwaltung (`account:*`)
  - AWS Aktiviere (`activate:*`)
  - AWS Artifact (`artifact:*`)
  - AWS Billing Conductor (`billingconductor:*`)
  - AWS Compute Optimizer (`compute-optimizer:*`)
  - AWS Data Pipeline (`datapipeline:GetAccountLimits`)
  - AWS Device Farm(`devicefarm:*`)
  - AWS Marketplace (`discovery-marketplace:*`)
  - Amazon ECR () `ecr-public:*`
  - AWS License Manager (`license-manager:ListReceivedLicenses`)
  - AWS Lichtsegel () `lightsail:Get*`
  - AWS Resource Explorer (`resource-explorer-2:*`)
  - Amazon S3 (`s3:CreateMultiRegionAccessPoint`,`s3:GetBucketPolicyStatus`) `s3:PutMultiRegionAccessPointPolicy`
  - AWS Sparpläne (`savingsplans:*`)
  - IAM-Identitätszentrum () `sso:*`
  - AWS Support App (`supportapp:*`)
  - Support Pläne () `supportplans:*`
  - AWS Nachhaltigkeit (`sustainability:*`)

- AWS Resource Groups Tagging API (`tag:GetResources`)
- AWS Marketplace Einblicke in Anbieter (`vendor-insights:ListEntitledSecurityProfiles`)

Proaktive Kontrollen im AWS Control Tower sind allgemein verfügbar

13. April 2023

(Für die AWS Control Tower-Landezone ist kein Update erforderlich.)

Proaktive Kontrollen im AWS Control Tower sind jetzt allgemein verfügbar. Proaktive Kontrollen helfen Ihnen dabei, bewährte Verfahren für Ihre AWS Ressourcen durchzusetzen. Weitere Informationen zu proaktiven Kontrollen finden Sie unter Proaktive Kontrollen.

Proaktive Kontrollen sind überall dort verfügbar AWS-Regionen , wo AWS Control Tower verfügbar ist. Eine Liste der Standorte AWS-Regionen , an denen AWS Control Tower verfügbar ist, finden Sie in der AWS-Region Tabelle.

Januar — Dezember 2022

Im Jahr 2022 veröffentlichte AWS Control Tower die folgenden Updates:

- Gleichzeitige Kontooperationen
- Factory-Anpassung des Kontos (AFC)
- Umfassende Kontrollen helfen bei AWS Bereitstellung und Verwaltung von Ressourcen
- Der Konformitätsstatus ist für alle sichtbar AWS Config Regeln
- API für Kontrollen und eine neue CloudFormation Ressource
- cFCT unterstützt das Löschen von Stack-Sets
- Benutzerdefinierte Aufbewahrung von Protokollen
- Role-Drift-Reparatur verfügbar
- AWS Control Tower-Landezone, Version 3.0
- Die Seite Organisation kombiniert Ansichten von Organisationseinheiten und Konten
- Vereinfachte Kontoerstellung und Registrierung
- AFT unterstützt die automatische Anpassung für gemeinsam genutzte AWS Control Tower-Konten

- Gleichzeitige Operationen für alle optionalen Steuerungen
- Bestehende Sicherheits- und Logging-Konten
- AWS Control Tower-Landingzone, Version 2.9
- AWS-Kontrollturm-Landezone, Version 2.8

Gleichzeitige Kontooperationen

16. Dezember 2022

(Für die AWS Control Tower-Landezone ist kein Update erforderlich.)

AWS Control Tower unterstützt jetzt gleichzeitige Aktionen in Account Factory. Sie können bis zu fünf (5) Konten gleichzeitig erstellen, aktualisieren oder registrieren. Reichen Sie nacheinander bis zu fünf Aktionen ein und sehen Sie sich den Abschlussstatus jeder Anfrage an, während Ihre Konten im Hintergrund fertig erstellt werden. So müssen Sie beispielsweise nicht mehr warten, bis jeder Vorgang abgeschlossen ist, bevor Sie ein anderes Konto aktualisieren oder eine gesamte Organisationseinheit (OU) erneut registrieren.

Factory-Anpassung des Kontos (AFC)

28. November 2022

(Für die AWS Control Tower-Landezone ist kein Update erforderlich.)

Mit der Account-Factory-Anpassung können Sie neue und bestehende Konten von der AWS Control Tower-Konsole aus anpassen. Diese neuen Anpassungsfunktionen bieten Ihnen die Flexibilität, Account-Blueprints zu definieren. Dabei handelt es sich um CloudFormation Vorlagen, die in einem speziellen Service Catalog-Produkt enthalten sind. Blueprints stellen vollständig maßgeschneiderte Ressourcen und Konfigurationen bereit. Sie können auch vordefinierte Blueprints verwenden, die von AWS Partnern erstellt und verwaltet werden und die Ihnen helfen, Konten an bestimmte Anwendungsfälle anzupassen.

Bisher unterstützte AWS Control Tower Account Factory keine Kontoanpassung in der Konsole. Mit diesem Update von Account Factory können Sie Kontoanforderungen vorab definieren und sie als Teil eines klar definierten Workflows implementieren. Sie können Blueprints anwenden, um neue Konten zu erstellen, andere AWS Konten bei AWS Control Tower zu registrieren und bestehende AWS Control Tower-Konten zu aktualisieren.

Wenn Sie ein Konto in Account Factory bereitstellen, registrieren oder aktualisieren, wählen Sie den Blueprint aus, der bereitgestellt werden soll. Die im Blueprint angegebenen Ressourcen werden in Ihrem Konto bereitgestellt. Wenn die Erstellung Ihres Kontos abgeschlossen ist, können alle benutzerdefinierten Konfigurationen sofort verwendet werden.

Um mit der Anpassung von Konten zu beginnen, können Sie die Ressourcen für Ihren beabsichtigten Anwendungsfall in einem Service Catalog-Produkt definieren. Sie können auch von Partnern verwaltete Lösungen aus der AWS Getting Started Library auswählen. Weitere Informationen finden Sie unter Passen Sie Konten mit Account Factory Customization (AFC) an.

Umfassende Kontrollen helfen bei AWS Bereitstellung und Verwaltung von Ressourcen

28. November 2022

(Für die AWS Control Tower-Landezone ist kein Update erforderlich.)

AWS Control Tower unterstützt jetzt ein umfassendes Kontrollmanagement, einschließlich neuer, optionaler proaktiver Kontrollen, die über CloudFormation Hooks implementiert werden. Diese Kontrollen werden als proaktiv bezeichnet, da sie Ihre Ressourcen — bevor die Ressourcen bereitgestellt werden — überprüfen, um festzustellen, ob die neuen Ressourcen den in Ihrer Umgebung aktivierten Kontrollen entsprechen.

Über 130 neue proaktive Kontrollen unterstützen Sie dabei, bestimmte politische Ziele für Ihre AWS Control Tower-Umgebung zu erreichen, die Anforderungen branchenüblicher Compliance-Frameworks zu erfüllen und die Interaktionen mit AWS Control Tower in mehr als zwanzig anderen AWS Services zu regeln.

Die Kontrollbibliothek von AWS Control Tower klassifiziert diese Kontrollen nach den zugehörigen AWS Diensten und Ressourcen. Weitere Informationen finden Sie unter Proaktive Kontrollen.

Mit dieser Version ist AWS Control Tower auch in den neuen Security Hub Service-Managed CSPM-Standard integriert: AWS Control Tower, der den Standard AWS Foundational Security Best Practices (FSBP) unterstützt. AWS Security Hub CSPM Sie können über 160 Security Hub CSPM-Steuerelemente zusammen mit den AWS Control Tower-Steuerelementen in der Konsole anzeigen, und Sie können einen Security Hub CSPM-Sicherheitswert für Ihre AWS Control Tower-Umgebung abrufen. Weitere Informationen finden Sie unter Security Hub-Steuerelemente. https://docs.aws.amazon.com/controltower/latest/controlreference/security-hub-controls.html

Der Konformitätsstatus ist für alle sichtbar AWS Config Regeln

18. November 2022

(Für die AWS Control Tower-Landezone ist kein Update erforderlich.)

AWS Control Tower zeigt jetzt den Konformitätsstatus aller AWS Config Regeln an, die in den bei AWS Control Tower registrierten Organisationseinheiten implementiert wurden. Sie können den Compliance-Status aller AWS Config Regeln einsehen, die sich auf Ihre Konten im AWS Control Tower auswirken, unabhängig davon, ob Sie registriert sind oder nicht, ohne die AWS Control Tower-Konsole verlassen zu müssen. Kunden können wählen, ob sie Config-Regeln, sogenannte Detective Controls, im AWS Control Tower einrichten oder sie direkt über den Service einrichten möchten. AWS Config Die von bereitgestellten Regeln AWS Config werden zusammen mit den vom AWS Control Tower bereitgestellten Regeln angezeigt.

Bisher waren AWS Config Regeln, die über den AWS Config Service bereitgestellt wurden, in der AWS Control Tower-Konsole nicht sichtbar. Kunden mussten zum AWS Config Service navigieren, um Regeln zu identifizieren, die nicht den AWS Config Vorschriften entsprechen. Jetzt können Sie jede nicht konforme AWS Config Regel in der AWS Control Tower-Konsole identifizieren. Um den Konformitätsstatus all Ihrer Config-Regeln einzusehen, navigieren Sie zur Seite mit den Kontodetails in der AWS Control Tower-Konsole. Sie sehen eine Liste mit dem Compliance-Status der vom AWS Control Tower verwalteten Kontrollen und der Config-Regeln, die außerhalb von AWS Control Tower bereitgestellt werden.

API für Kontrollen und eine neue CloudFormation Ressource

1. September 2022

(Für die AWS Control Tower-Landezone ist kein Update erforderlich.)

AWS Control Tower unterstützt jetzt die programmatische Verwaltung von Kontrollen, auch bekannt als Guardrails, über eine Reihe von API-Aufrufen. Eine neue CloudFormation Ressource unterstützt die API-Funktionalität für Steuerelemente. Weitere Informationen finden Sie unter Automatisieren Sie Aufgaben im AWS Control Tower und Create AWS Control Tower Ressourcen mit AWS CloudFormation.

Mit diesen APIs können Sie Steuerelemente in der AWS Control Tower-Bibliothek aktivieren, deaktivieren und deren Anwendungsstatus anzeigen. Die APIs bieten Unterstützung für CloudFormation, sodass Sie AWS Ressourcen als Infrastructure-as-Code (IaC) verwalten können. AWS Control Tower bietet optionale präventive und detektivische Kontrollen, die Ihre politischen

Absichten in Bezug auf eine gesamte Organisationseinheit (OU) und jedes Konto innerhalb der OU zum Ausdruck bringen. AWS Diese Regeln bleiben in Kraft, wenn Sie neue Konten erstellen oder Änderungen an bestehenden Konten vornehmen.

In dieser Version enthaltene APIs

- EnableControl— Dieser API-Aufruf aktiviert ein Steuerelement. Es startet einen asynchronen Vorgang, der AWS Ressourcen für die angegebene Organisationseinheit und die darin enthaltenen Konten erstellt.
- DisableControl— Dieser API-Aufruf schaltet ein Steuerelement aus. Es startet einen asynchronen Vorgang, der AWS Ressourcen in der angegebenen Organisationseinheit und den darin enthaltenen Konten löscht.
- GetControlOperation— Gibt den Status einer bestimmten EnableControl OR-Operation zurück. DisableControl
- ListEnabledControls— Listet die von AWS Control Tower aktivierten Kontrollen für die angegebene Organisationseinheit und die darin enthaltenen Konten auf.

Eine Liste der Kontrollnamen für optionale Steuerelemente finden Sie unter Resource Identifiers for APIs and Controls im AWS Control Tower-Benutzerhandbuch.

cFCT unterstützt das Löschen von Stack-Sets

26. August 2022

(Für die AWS Control Tower-Landezone ist kein Update erforderlich.)

Anpassungen für AWS Control Tower (cFCT) unterstützen jetzt das Löschen von Stack-Sets, indem ein Parameter in der `manifest.yaml` Datei festgelegt wird. Weitere Informationen finden Sie unter Löschen eines Stack-Sets.

> **Important**
>
> Wenn Sie den Wert von anfänglich `enable_stack_set_deletion` auf setzen`true`, werden beim nächsten Aufruf von cFCT ALLE Ressourcen, die mit dem Präfix beginnen`CustomControlTower-`, das zugehörige Schlüssel-Tag `Key:AWS_Solutions, Value: CustomControlTowerStackSet` haben und die nicht in der Manifestdatei deklariert sind, zum Löschen bereitgestellt.

Benutzerdefinierte Aufbewahrung von Protokollen

15. August 2022

(Für die Landezone des AWS Control Tower ist ein Update erforderlich. Weitere Informationen finden Sie unterAktualisiere deine landing zone)

AWS Control Tower bietet jetzt die Möglichkeit, die Aufbewahrungsrichtlinie für Amazon S3-Buckets anzupassen, in denen Ihre AWS Control CloudTrail Tower-Protokolle gespeichert werden. Sie können Ihre Amazon S3-Aufbewahrungsrichtlinie für Protokolle in Schritten von Tagen oder Jahren, bis zu einem Maximum von 15 Jahren, anpassen.

Wenn Sie Ihre Protokollspeicherung nicht anpassen möchten, sind die Standardeinstellungen 1 Jahr für die Standardkontoprotokollierung und 10 Jahre für die Zugriffsprotokollierung.

Diese Funktion ist für Bestandskunden über den AWS Control Tower verfügbar, wenn Sie Ihre Landing Zone aktualisieren oder reparieren, und für Neukunden über das AWS Control Tower-Setup

Role-Drift-Reparatur verfügbar

11. August 2022

(Für die AWS Control Tower-Landezone ist kein Update erforderlich.)

AWS Control Tower unterstützt jetzt die Reparatur von Rollenabweichungen. Sie können eine erforderliche Rolle wiederherstellen, ohne Ihre Landezone vollständig reparieren zu müssen. Falls diese Art der Drift-Reparatur erforderlich ist, finden Sie auf der Konsolen-Fehlerseite Schritte zum Wiederherstellen der Rolle, sodass Ihre Landing Zone wieder verfügbar ist.

AWS Control Tower-Landezone, Version 3.0

29. Juli 2022

(Für die AWS Control Tower-Landezone auf Version 3.0 ist ein Update erforderlich. Weitere Informationen finden Sie unterAktualisiere deine landing zone)

Die Version 3.0 der AWS Control Tower-Landing Zone umfasst die folgenden Updates:

- Die Option, AWS CloudTrail Trails auf Organisationsebene auszuwählen oder sich von den vom AWS Control Tower verwalteten CloudTrail Trails abzumelden.

- Zwei neue Detektivkontrollen, mit denen festgestellt werden kann, ob AWS CloudTrail Aktivitäten in Ihren Konten protokolliert werden.
- Die Option, AWS Config Informationen über globale Ressourcen nur in Ihrer Heimatregion zu aggregieren.
- Ein Update zum Thema Region Deny Control.
- Ein Update der verwalteten Richtlinie, AWSControlTowerServiceRolePolicy.
- Wir erstellen die IAM-Rolle `aws-controltower-CloudWatchLogsRole` und die CloudWatch Protokollgruppe nicht mehr `aws-controltower/CloudTrailLogs` in jedem registrierten Konto. Bisher haben wir diese in jedem Konto für den zugehörigen Account-Trail erstellt. Bei Organisationspfaden erstellen wir nur einen im Verwaltungskonto.

In den folgenden Abschnitten finden Sie weitere Informationen zu jeder neuen Funktion.

Organization-level CloudTrail Pfade im AWS Control Tower

Mit der Landing Zone-Version 3.0 unterstützt der AWS Control Tower jetzt Pfade auf Organisationsebene AWS CloudTrail .

Wenn Sie Ihre AWS Control Tower-Landingzone auf Version 3.0 aktualisieren, haben Sie die Möglichkeit, AWS CloudTrail Trails auf Organisationsebene als Ihre bevorzugte Protokollierung auszuwählen oder CloudTrail Trails, die von AWS Control Tower verwaltet werden, abzulehnen. Wenn Sie auf Version 3.0 aktualisieren, löscht AWS Control Tower die vorhandenen Trails auf Kontoebene für registrierte Konten nach einer Wartezeit von 24 Stunden. AWS Control Tower löscht keine Trails auf Kontoebene für Konten, die noch nicht registriert sind. In dem unwahrscheinlichen Fall, dass Ihr Landing Zone-Update nicht erfolgreich ist, der Fehler jedoch auftritt, nachdem AWS Control Tower den Trail auf Organisationsebene bereits erstellt hat, können Ihnen doppelte Gebühren für Trails auf Organisations- und Kontoebene entstehen, bis Ihr Aktualisierungsvorgang erfolgreich abgeschlossen werden kann.

Ab Landing Zone 3.0 unterstützt der AWS Control Tower keine Trails mehr auf Kontoebene, die verwaltet werden. AWS Stattdessen erstellt AWS Control Tower einen Trail auf Organisationsebene, der je nach Ihrer Auswahl aktiv oder inaktiv ist.

> **Note**
>
> Nach dem Update auf Version 3.0 oder höher haben Sie nicht die Möglichkeit, mit den von AWS Control Tower verwalteten CloudTrail Trails auf Kontoebene fortzufahren.

Aus Ihren aggregierten Kontoprotokollen gehen keine Protokolldaten verloren, da die Protokolle im vorhandenen Amazon S3-Bucket verbleiben, in dem sie gespeichert sind. Nur die Trails werden gelöscht, nicht die vorhandenen Logs. Wenn Sie die Option zum Hinzufügen von Protokollen auf Organisationsebene auswählen, öffnet AWS Control Tower einen neuen Pfad zu einem neuen Ordner in Ihrem Amazon S3-Bucket und sendet weiterhin Protokollierungsinformationen an diesen Speicherort. Wenn Sie sich dafür entscheiden, die vom AWS Control Tower verwalteten Trails abzulehnen, bleiben Ihre vorhandenen Logs unverändert im Bucket.

Konventionen zur Pfadbenennung für die Speicherung von Protokollen

- Konto-Trail-Logs werden mit einem Pfad in der folgenden Form gespeichert: `/org id/AWSLogs/…`
- Organisations-Traillogs werden mit einem Pfad in der folgenden Form gespeichert: `/org id/AWSLogs/org id/…`

Der Pfad, den AWS Control Tower für Ihre CloudTrail Pfade auf Organisationsebene erstellt, unterscheidet sich vom Standardpfad für einen manuell erstellten Pfad auf Organisationsebene, der das folgende Format haben würde:

- `/AWSLogs/org id/…`

Weitere Informationen zur CloudTrail Pfadbenennung finden Sie unter Suchen Ihrer Protokolldateien. CloudTrail

> **Tip**
>
> Wenn Sie vorhaben, Ihre eigenen Trails auf Kontoebene zu erstellen und zu verwalten, empfehlen wir Ihnen, die neuen Trails zu erstellen, bevor Sie das Update auf die AWS Control Tower Landing Zone Version 3.0 abschließen, um sofort mit der Protokollierung zu beginnen.

Sie können sich jederzeit dafür entscheiden, neue CloudTrail Trails auf Konto- oder Organisationsebene zu erstellen und diese selbst zu verwalten. Die Option, CloudTrail Trails auf Organisationsebene auszuwählen, die vom AWS Control Tower verwaltet werden, ist bei jedem Landing Zone-Update auf Version 3.0 oder höher verfügbar. Sie können sich bei jeder Aktualisierung Ihrer Landezone für Trails auf Organisationsebene an- und abmelden.

Wenn deine Logs von einem Drittanbieter-Dienst verwaltet werden, gib unbedingt den neuen Pfadnamen für deinen Dienst an.

> **Note**
>
> Für Landezonen der Version 3.0 oder höher werden AWS CloudTrail Trails auf Kontoebene vom AWS Control Tower nicht unterstützt. Sie können jederzeit Ihre eigenen Trails auf Kontoebene erstellen und verwalten, oder Sie können sich für Trails auf Organisationsebene entscheiden, die vom AWS Control Tower verwaltet werden.

Erfassen Sie nur AWS Config Ressourcen in der Heimatregion

In der Landing Zone-Version 3.0 hat AWS Control Tower die Basiskonfiguration für aktualisiert, AWS Config sodass nur globale Ressourcen in der Heimatregion aufgezeichnet werden. Nach dem Update auf Version 3.0 ist die Ressourcenaufzeichnung für globale Ressourcen nur in Ihrer Heimatregion aktiviert.

Diese Konfiguration wird als bewährte Methode angesehen. Sie wird von AWS Security Hub CSPM und empfohlen und führt zu Kosteneinsparungen AWS Config, da die Anzahl der Konfigurationselemente reduziert wird, die beim Erstellen, Ändern oder Löschen globaler Ressourcen erstellt werden. Bisher wurde jedes Mal, wenn eine globale Ressource erstellt, aktualisiert oder gelöscht wurde, sei es durch einen Kunden oder durch einen AWS Service, ein Konfigurationselement für jedes Element in jeder regulierten Region erstellt.

Zwei neue Detektivsteuerungen für die AWS CloudTrail Protokollierung

Im Rahmen der Umstellung auf Organisationsebenen AWS CloudTrail führt AWS Control Tower zwei neue Detektivkontrollen ein, die überprüfen, ob sie aktiviert CloudTrail sind. Für die erste Kontrolle ist eine obligatorische Anleitung erforderlich. Sie wird in der Sicherheits-Organisationseinheit bei der Einrichtung oder bei Aktualisierungen der Landezone von Version 3.0 und höher aktiviert. Für die zweite Kontrolle gilt die Empfehlung „Dringend empfohlen“. Sie wird optional auf alle Organisationseinheiten angewendet, mit Ausnahme der Sicherheits-OU, für die der obligatorische Kontrollschutz bereits durchgesetzt wurde.

Obligatorische Kontrolle: Ermitteln Sie, ob für gemeinsame Konten der Organisationseinheit Security AWS CloudTrail oder CloudTrail Lake aktiviert ist

Dringend empfohlene Kontrolle: Ermitteln Sie, ob für ein Konto AWS CloudTrail oder CloudTrail Lake aktiviert ist

Weitere Informationen zu den neuen Steuerelementen finden Sie unter The AWS Control Tower Controls Library.

Ein Update für die Region Deny Control

Wir haben die NotAction Liste in der Region „Kontrolle verweigern“ um Aktionen einiger zusätzlicher Dienste aktualisiert, die unten aufgeführt sind:

```
"chatbot:*",
"s3:GetAccountPublic",
"s3:DeleteMultiRegionAccessPoint",
"s3:DescribeMultiRegionAccessPointOperation",
"s3:GetMultiRegionAccessPoint",
"s3:GetMultiRegionAccessPointPolicy",
"s3:GetMultiRegionAccessPointPolicyStatus",
"s3:ListMultiRegionAccessPoints",
"s3:GetStorageLensConfiguration",
"s3:GetStorageLensDashboard",
"s3:ListStorageLensConfigurations"
"s3:GetAccountPublicAccessBlock",
"s3:PutAccountPublic",
"s3:PutAccountPublicAccessBlock",
```

Video-Anleitung

Dieses Video (3:07) beschreibt, wie Sie Ihre bestehende AWS Control Tower-Landezone auf Version 3 aktualisieren. Wählen Sie zur besseren Ansicht das Symbol in der rechten unteren Ecke des Videos, um es in voller Bildschirmgröße anzuzeigen. Es stehen Untertitel zur Verfügung.

Video-Walkthrough zur Aktualisierung einer bestehenden AWS Control Tower-Landezone auf Landezone 3.

Die Seite Organisation kombiniert Ansichten von Organisationseinheiten und Konten

18. Juli 2022

(Für die AWS Control Tower-Landezone ist kein Update erforderlich)

Die neue Organisationsseite in AWS Control Tower zeigt eine hierarchische (Baum-) Ansicht aller Organisationseinheiten (OUs) und Konten. Sie kombiniert die Informationen aus den Seiten OUs und Accounts, die zuvor existierten.

Auf der neuen Seite sehen Sie die Beziehungen zwischen übergeordneten Organisationseinheiten und ihren verschachtelten Organisationseinheiten und Konten. Sie können Maßnahmen für Gruppierungen von Ressourcen ergreifen. Sie können die Seitenansicht konfigurieren. Sie können beispielsweise die hierarchische Ansicht erweitern oder reduzieren, die Ansicht so filtern, dass nur Konten oder Organisationseinheiten angezeigt werden, dass nur Ihre registrierten Konten und registrierten Organisationseinheiten angezeigt werden, oder Sie können Gruppen verwandter Ressourcen anzeigen. Es ist einfacher sicherzustellen, dass Ihre gesamte Organisation ordnungsgemäß aktualisiert wird.

Vereinfachte Kontoerstellung und Registrierung

30. Juni 2022

(Für die AWS Control Tower-Landezone ist kein Update erforderlich.)

AWS Control Tower bietet jetzt einen vereinfachten Arbeitsablauf für die Erstellung und Registrierung von Konten. Sie können in einem einzigen Workflow ein neues Konto erstellen oder ein vorhandenes Konto registrieren, ohne zur Service Catalog-Konsole zu navigieren. Weitere Informationen finden Sie unter Registrieren Sie ein vorhandenes Konto über die AWS Control Tower-Konsole.

AFT unterstützt die automatische Anpassung für gemeinsam genutzte AWS Control Tower-Konten

27. Mai 2022

(Für die AWS Control Tower-Landezone ist kein Update erforderlich)

Account Factory for Terraform (AFT) kann jetzt alle Ihre Konten, die von AWS Control Tower verwaltet werden, programmgesteuert anpassen und aktualisieren, einschließlich des Verwaltungskontos, des Auditkontos und des Protokollarchivkontos, zusammen mit Ihren registrierten Konten. Sie können Ihre Kontoanpassungs- und Aktualisierungsverwaltung zentralisieren und gleichzeitig die Sicherheit Ihrer Kontokonfigurationen schützen, da Sie die Rolle festlegen, die die Arbeit ausführt.

Die bestehende AWSaftExecution-Rolle stellt jetzt Anpassungen in allen Konten bereit. Sie können IAM-Berechtigungen mit Grenzen einrichten, die den Zugriff auf die AWSaftExecution-

Rolle entsprechend Ihren Geschäfts- und Sicherheitsanforderungen einschränken. Sie können die genehmigten Anpassungsberechtigungen in dieser Rolle für vertrauenswürdige Benutzer auch programmgesteuert delegieren. Als bewährte Methode empfehlen wir, die Berechtigungen auf diejenigen zu beschränken, die für die Bereitstellung der erforderlichen Anpassungen erforderlich sind.

AFT erstellt jetzt die neue AWSAftService-Rolle, um AFT-Ressourcen in allen verwalteten Konten bereitzustellen, einschließlich der gemeinsamen Konten und des Verwaltungskontos. Ressourcen wurden früher von der AWSaftExecution-Rolle bereitgestellt.

Die gemeinsamen Konten und Verwaltungskonten für AWS Control Tower werden nicht über Account Factory bereitgestellt, sodass für sie keine entsprechenden bereitgestellten Produkte vorhanden sind. AWS Service Catalog Daher können Sie die gemeinsamen Konten und Verwaltungskonten in Service Catalog nicht aktualisieren.

Gleichzeitige Operationen für alle optionalen Steuerungen

18. Mai 2022

(Für die AWS Control Tower-Landezone ist kein Update erforderlich)

Der AWS Control Tower unterstützt jetzt gleichzeitige Operationen für präventive Kontrollen sowie für detektivische Kontrollen.

Mit dieser neuen Funktion kann jede optionale Steuerung jetzt gleichzeitig angewendet oder entfernt werden, wodurch die Benutzerfreundlichkeit und Leistung aller optionalen Kontrollen verbessert werden. Sie können mehrere optionale Steuerungen aktivieren, ohne auf den Abschluss einzelner Steuervorgänge warten zu müssen. Die einzigen eingeschränkten Zeiten sind, wenn der AWS Control Tower gerade dabei ist, eine Landezone einzurichten, oder wenn die Verwaltung auf eine neue Organisation ausgedehnt wird.

Unterstützte Funktionen für präventive Kontrollen:

- Wenden Sie verschiedene präventive Kontrollen auf derselben Organisationseinheit an und entfernen Sie sie.
- Gleichzeitiges Anwenden und Entfernen verschiedener präventiver Kontrollen auf verschiedenen Organisationseinheiten
- Wenden Sie dieselbe präventive Kontrolle gleichzeitig auf mehreren Organisationseinheiten an und entfernen Sie sie.

- Sie können alle präventiven und detektivischen Kontrollen gleichzeitig anwenden und entfernen.

Sie können diese Verbesserungen bei der Kontrolle der Parallelität in allen veröffentlichten Versionen von AWS Control Tower erleben.

Wenn Sie präventive Kontrollen auf verschachtelte Organisationseinheiten anwenden, wirken sich die präventiven Kontrollen auf alle Konten und Organisationseinheiten aus, die unter der Ziel-Organisationseinheit verschachtelt sind, auch wenn diese Konten und Organisationseinheiten nicht bei AWS Control Tower registriert sind. Präventive Kontrollen werden mithilfe von Service Control Policies (SCPs) implementiert, die Teil von sind. AWS Organizations Detektivkontrollen werden mithilfe von AWS Config Regeln implementiert. Die Richtlinien bleiben in Kraft, wenn Sie neue Konten erstellen oder Änderungen an Ihren bestehenden Konten vornehmen, und AWS Control Tower bietet einen zusammenfassenden Bericht darüber, wie jedes Konto Ihren aktivierten Richtlinien entspricht. Eine vollständige Liste der verfügbaren Steuerelemente finden Sie in der Kontrollbibliothek für den AWS Control Tower.

Bestehende Sicherheits- und Logging-Konten

16. Mai 2022

(Bei der Ersteinrichtung verfügbar.)

AWS Control Tower bietet Ihnen jetzt die Möglichkeit, bei der ersten Einrichtung der Landezone ein vorhandenes AWS Konto als AWS Control Tower-Sicherheits- oder Logging-Konto anzugeben. Mit dieser Option muss AWS Control Tower keine neuen, gemeinsam genutzten Konten erstellen. Das Sicherheitskonto, das standardmäßig Audit-Konto genannt wird, ist ein eingeschränktes Konto, das Ihren Sicherheits- und Compliance-Teams Zugriff auf alle Konten in Ihrer Landezone gewährt. Das Logging-Konto, das standardmäßig als Log-Archive-Konto bezeichnet wird, dient als Repository. Es speichert Protokolle der API-Aktivitäten und Ressourcenkonfigurationen von allen Konten in Ihrer Landing Zone.

Indem Sie Ihre vorhandenen Sicherheits- und Logging-Konten verwenden, ist es einfacher, die AWS Control Tower-Governance auf Ihre bestehenden Organisationen auszudehnen oder von einer alternativen Landezone zum AWS Control Tower zu wechseln. Die Option, vorhandene Konten zu verwenden, wird Ihnen bei der ersten Einrichtung der Landezone angezeigt. Sie umfasst Prüfungen während des Einrichtungsvorgangs, die eine erfolgreiche Bereitstellung sicherstellen. AWS Control Tower implementiert die erforderlichen Rollen und Kontrollen für Ihre bestehenden Konten. Es entfernt oder führt keine vorhandenen Ressourcen oder Daten zusammen, die in diesen Konten vorhanden sind.

Einschränkung: Wenn Sie beabsichtigen, bestehende AWS Konten als Prüf- und Protokollarchivierungskonten in den AWS Control Tower zu integrieren, und wenn diese Konten über vorhandene AWS Config Ressourcen verfügen, müssen Sie die vorhandenen AWS Config Ressourcen löschen, bevor Sie die Konten bei AWS Control Tower registrieren können.

AWS Control Tower-Landingzone, Version 2.9

22. April 2022

(Für die Landing Zone des AWS Control Tower auf Version 2.9 ist ein Update erforderlich. Weitere Informationen finden Sie unterAktualisiere deine landing zone)

Die AWS Control Tower Landing Zone Version 2.9 aktualisiert den Notification Forwarder Lambda so, dass er die Python-Laufzeit der Version 3.9 verwendet. Dieses Update behebt die veraltete Python-Version 3.6, die für Juli 2022 geplant ist. Die neuesten Informationen finden Sie auf der Seite zur Python-Veralterung.

AWS-Kontrollturm-Landezone, Version 2.8

10. Februar 2022

(Für die Landing Zone des AWS Control Tower auf Version 2.8 ist ein Update erforderlich. Weitere Informationen finden Sie unterAktualisiere deine landing zone)

Die AWS Control Tower Landing Zone Version 2.8 bietet Funktionen, die den jüngsten Aktualisierungen der AWS grundlegenden Best Practices für Sicherheit entsprechen.

In dieser Version:

- Die Zugriffsprotokollierung ist für den Zugriffs-Log-Bucket im Log-Archive-Konto konfiguriert, um den Zugriff auf den vorhandenen S3-Zugriffsprotokoll-Bucket zu verfolgen.
- Unterstützung für Lifecycle-Richtlinien wurde hinzugefügt. Das Zugriffsprotokoll für den vorhandenen S3-Zugriffsprotokoll-Bucket ist auf eine Standardaufbewahrungszeit von 10 Jahren festgelegt.
- Darüber hinaus aktualisiert diese Version AWS Control Tower so, dass die AWS Service Linked Role (SLR), die von bereitgestellt wird AWS Config, in allen verwalteten Konten (ohne das Verwaltungskonto) verwendet wird, sodass Sie Config-Regeln einrichten und verwalten können, die den AWS Config Best Practices entsprechen. Kunden, die kein Upgrade durchführen, verwenden weiterhin ihre bestehende Rolle.

- Diese Version optimiert den AWS Control Tower KMS-Konfigurationsprozess für die Verschlüsselung von AWS Config Daten und verbessert die zugehörigen Statusmeldungen in. CloudTrail
- Die Version beinhaltet ein Update für Region Deny Control, um die Nutzung der `route53-application-recovery` Funktion zu ermöglichen. `us-west-2`
- Update: Am 15. Februar 2022 haben wir die Warteschlange für unzustellbare Nachrichten für AWS Lambda-Funktionen entfernt.

Weitere Details:

- Wenn Sie Ihre Landezone außer Betrieb nehmen, entfernt AWS Control Tower die AWS Config serviceverknüpfte Rolle nicht.
- Wenn Sie die Bereitstellung eines Account Factory-Kontos aufheben, entfernt AWS Control Tower die mit dem AWS Config Service verknüpfte Rolle nicht.

Um Ihre Landing Zone auf 2.8 zu aktualisieren, navigieren Sie zur Seite mit den Landing Zone-Einstellungen, wählen Sie die Version 2.8 aus und wählen Sie dann Update aus. Nachdem Sie Ihre Landing Zone aktualisiert haben, müssen Sie alle Konten aktualisieren, die vom AWS Control Tower verwaltet werden, wie unter beschriebenVerwaltung von Konfigurationsupdates in AWS Control Tower.

Januar — Dezember 2021

Im Jahr 2021 veröffentlichte AWS Control Tower die folgenden Updates:

- Funktionen zur Sperrung von Regionen
- Funktionen zur Datenresidenz
- AWS Control Tower führt die Bereitstellung und Anpassung von Terraform-Konten ein
- Neues Lifecycle-Ereignis verfügbar
- AWS Control Tower ermöglicht verschachtelte OUs
- Parallelität bei der Detektivkontrolle
- Zwei neue Regionen verfügbar
- Abwahl der Region
- AWS Control Tower funktioniert mit AWS Wichtige Managementsysteme

- Steuerung umbenannt, Funktionalität unverändert
- Der AWS Control Tower scannt täglich SCPs, um nach Abweichungen zu suchen
- Benutzerdefinierte Namen für Organisationseinheiten und Konten
- AWS Control Tower-Landezone, Version 2.7
- Drei neue AWS Regionen verfügbar
- Nur ausgewählte Regionen verwalten
- AWS Control Tower dehnt die Governance jetzt auf bestehende Organisationseinheiten in Ihrem Unternehmen aus AWS Organisationen
- AWS Control Tower bietet massenweise Kontoaktualisierungen

Funktionen zur Sperrung von Regionen

30. November 2021

(Für die AWS Control Tower-Landezone ist kein Update erforderlich.)

AWS Control Tower bietet jetzt Funktionen zum Verweigern von Regionen, mit denen Sie den Zugriff auf AWS Dienste und Abläufe für registrierte Konten in Ihrer AWS Control Tower-Umgebung einschränken können. Die Funktion „Region verweigern“ ergänzt die vorhandenen Funktionen zur Regionsauswahl und zur Abwahl von Regionen im AWS Control Tower. Zusammen helfen Ihnen diese Funktionen dabei, Compliance- und regulatorische Bedenken zu lösen und gleichzeitig die Kosten auszugleichen, die mit der Expansion in weitere Regionen verbunden sind.

Beispielsweise können AWS Kunden in Deutschland den Zugang zu AWS Diensten in Regionen außerhalb der Region Frankfurt verweigern. Sie können eingeschränkte Regionen während der Einrichtung des AWS Control Tower oder auf der Seite mit den Landing Zone-Einstellungen auswählen. Die Funktion „Region verweigern“ ist verfügbar, wenn Sie Ihre AWS Control Tower-Landingzone-Version aktualisieren. Ausgewählte AWS Services sind von der Funktion „Region verweigern“ ausgenommen. Weitere Informationen finden Sie unter „Region Deny Control“ konfigurieren.

Funktionen zur Datenresidenz

30. November 2021

(Für die AWS Control Tower-Landezone ist kein Update erforderlich)

AWS Control Tower bietet jetzt speziell entwickelte Steuerelemente, mit denen Sie sicherstellen können, dass sich alle Kundendaten, die Sie in AWS Services hochladen, nur in den von Ihnen AWS angegebenen Regionen befinden. Sie können die AWS Region oder Regionen auswählen, in denen Ihre Kundendaten gespeichert und verarbeitet werden. Eine vollständige Liste der AWS Regionen, in denen AWS Control Tower verfügbar ist, finden Sie AWS in der Regionentabelle.

Für eine detaillierte Steuerung können Sie zusätzliche Steuerelemente anwenden, z. B. Amazon Virtual Private Network (VPN) -Verbindungen verbieten oder Internetzugriff für eine Amazon VPC-Instance verbieten. Sie können den Konformitätsstatus der Kontrollen in der AWS Control Tower-Konsole einsehen. Eine vollständige Liste der verfügbaren Kontrollen finden Sie in der Kontrollbibliothek für den AWS Control Tower.

AWS Control Tower führt die Bereitstellung und Anpassung von Terraform-Konten ein

29. November 2021

(Optionales Update für die AWS Control Tower-Landezone)

Mit AWS Control Tower Account Factory for Terraform (AFT) können Sie jetzt Terraform verwenden, um benutzerdefinierte Konten über AWS Control Tower bereitzustellen und zu aktualisieren.

AFT bietet eine einzige Terraform-Pipeline (Infrastructure as Code, IaC), die von AWS Control Tower verwaltete Konten bereitstellt. Anpassungen während der Bereitstellung helfen dabei, Ihre Geschäfts- und Sicherheitsrichtlinien einzuhalten, bevor Sie die Konten an Endbenutzer weitergeben.

Die automatische AFT-Pipeline zur Kontoerstellung überwacht, bis die Kontobereitstellung abgeschlossen ist. Anschließend wird sie fortgesetzt und zusätzliche Terraform-Module ausgelöst, die das Konto um alle erforderlichen Anpassungen erweitern. Als zusätzlichen Teil des Anpassungsprozesses können Sie die Pipeline so konfigurieren, dass Ihre eigenen benutzerdefinierten Terraform-Module installiert werden, und Sie können wählen, ob Sie eine der AFT-Funktionsoptionen hinzufügen möchten, die von für allgemeine Anpassungen bereitgestellt werden. AWS

Beginnen Sie mit AWS Control Tower Account Factory für Terraform, indem Sie die Schritte im AWS Control Tower-Benutzerhandbuch befolgen und AFT für Ihre Stellen Sie AWS Control Tower Account Factory für Terraform (AFT) bereit Terraform-Instance herunterladen. AFT unterstützt die Open-Source-Distributionen Terraform Cloud, Terraform Enterprise und Terraform.

Neues Lifecycle-Ereignis verfügbar

18. November 2021

(Für die Landungszone des AWS Control Tower ist kein Update erforderlich)

Das `PrecheckOrganizationalUnit` Ereignis protokolliert, ob Ressourcen den Erfolg der Extend-Governance-Aufgabe blockieren, einschließlich Ressourcen in verschachtelten Organisationseinheiten. Weitere Informationen finden Sie unter `PrecheckOrganizationalUnit`.

AWS Control Tower ermöglicht verschachtelte OUs

16. November 2021

(Für die AWS Control Tower-Landezone ist kein Update erforderlich)

Mit AWS Control Tower können Sie jetzt verschachtelte Organisationseinheiten als Teil Ihrer Landezone hinzufügen.

AWS Control Tower unterstützt verschachtelte Organisationseinheiten (OUs), sodass Sie Konten in mehrere Hierarchieebenen einteilen und präventive Kontrollen hierarchisch durchsetzen können. Sie können Organisationseinheiten registrieren, die verschachtelte Organisationseinheiten enthalten, Organisationseinheiten unter übergeordneten Organisationseinheiten erstellen und registrieren und Steuerungen für jede registrierte Organisationseinheit aktivieren, unabhängig von deren Tiefe. Um diese Funktion zu unterstützen, zeigt die Konsole die Anzahl der verwalteten Konten und Organisationseinheiten an.

Mit verschachtelten Organisationseinheiten können Sie Ihre AWS Control Tower-OUs an die Strategie mit AWS mehreren Konten ausrichten. Außerdem können Sie den Zeitaufwand für die Aktivierung von Kontrollen auf mehreren Organisationseinheiten reduzieren, indem Sie Kontrollen auf der Ebene der übergeordneten Organisationseinheit durchsetzen.

Wesentliche Überlegungen

1. Sie können bestehende, mehrstufige Organisationseinheiten nacheinander bei AWS Control Tower registrieren, wobei Sie mit der Organisationseinheit der obersten Ebene beginnen und dann in der Struktur nach unten fortschreiten. Weitere Informationen finden Sie unter Erweitern Sie von der flachen OU-Struktur zur verschachtelten OU-Struktur.
2. Konten, die direkt unter einer registrierten OU stehen, werden automatisch registriert. Konten, die sich weiter unten in der Struktur befinden, können registriert werden, indem ihre unmittelbare übergeordnete Organisationseinheit registriert wird.

3. Präventive Kontrollen (SCPs) werden automatisch in der Hierarchie nach unten vererbt. SCPs, die auf die übergeordnete Organisationseinheit angewendet werden, werden von allen verschachtelten Organisationseinheiten vererbt.
4. Detective Controls (AWS Config-Regeln) werden NICHT automatisch vererbt.
5. Die Einhaltung der Detektivkontrollen wird von jeder Organisationseinheit gemeldet.
6. Die SCP-Abweichung in einer OU wirkt sich auf alle Konten und Organisationseinheiten aus, die ihr unterstehen.
7. Sie können keine neuen verschachtelten Organisationseinheiten unter der Sicherheits-OU (Core-OU) erstellen.

Parallelität bei der Detektivkontrolle

5. November 2021

(Optionales Update für die AWS Control Tower-Landezone)

AWS Control Tower Detective Controls unterstützt jetzt gleichzeitige Operationen für detektivische Kontrollen und verbessert so die Benutzerfreundlichkeit und Leistung. Sie können mehrere Detektivkontrollen aktivieren, ohne auf den Abschluss einzelner Kontrollvorgänge warten zu müssen.

Unterstützte Funktionen:

- Aktivieren Sie verschiedene Detective Controls auf derselben OU (z. B. Ermitteln, ob MFA für den Root-Benutzer aktiviert ist, und Ermitteln, ob öffentlicher Schreibzugriff auf Amazon S3-Buckets zulässig ist).
- Aktivieren Sie gleichzeitig verschiedene Detective Controls auf verschiedenen Organisationseinheiten.
- Die Guardrail-Fehlermeldungen wurden verbessert und bieten nun zusätzliche Hinweise für unterstützte Operationen zur gleichzeitigen Steuerung.

In dieser Version nicht unterstützt:

- Die gleichzeitige Aktivierung derselben Detective Control auf mehreren Organisationseinheiten wird nicht unterstützt.
- Die gleichzeitige Verwendung präventiver Kontrollen wird nicht unterstützt.

Sie können die Verbesserungen der Parallelität bei der Detektivkontrolle in allen Versionen von AWS Control Tower erleben. Es wird empfohlen, dass Kunden, die derzeit nicht Version 2.7 verwenden, ein Landing Zone-Update durchführen, um die Vorteile anderer Funktionen nutzen zu können, wie z. B. die Auswahl und Abwahl von Regionen, die in der neuesten Version verfügbar sind.

Zwei neue Regionen verfügbar

29. Juli 2021

(Update für die Landungszone des AWS Control Tower erforderlich)

AWS Control Tower ist jetzt in zwei weiteren AWS Regionen verfügbar: Südamerika (Sao Paulo) und Europa (Paris). Dieses Update erweitert die Verfügbarkeit von AWS Control Tower auf 15 AWS Regionen.

Wenn Sie AWS Control Tower noch nicht kennen, können Sie es sofort in jeder der unterstützten Regionen starten. Während des Starts können Sie die Regionen auswählen, in denen AWS Control Tower Ihre Umgebung mit mehreren Konten aufbauen und verwalten soll.

Wenn Sie bereits über eine AWS Control Tower-Umgebung verfügen und die Governance-Funktionen von AWS Control Tower in einer oder mehreren unterstützten Regionen erweitern oder entfernen möchten, rufen Sie in Ihrem AWS Control Tower-Dashboard die Seite mit den Landing Zone-Einstellungen auf und wählen Sie dann die Regionen aus. Nachdem Sie Ihre Landing Zone aktualisiert haben, müssen Sie alle Konten aktualisieren, die vom AWS Control Tower verwaltet werden.

Abwahl der Region

29. Juli 2021

(Optionales Update für die AWS Control Tower-Landezone)

Die Abwahl der AWS-Control-Tower-Region verbessert Ihre Fähigkeit, die geografische Präsenz Ihrer AWS Control Tower-Ressourcen zu verwalten. Sie können die Auswahl von Regionen aufheben, die nicht mehr vom AWS Control Tower verwaltet werden sollen. Diese Funktion bietet Ihnen die Möglichkeit, Compliance- und regulatorische Bedenken zu berücksichtigen und gleichzeitig die Kosten abzuwägen, die mit der Expansion in weitere Regionen verbunden sind.

Die Abwahl der Region ist verfügbar, wenn Sie Ihre AWS Control Tower-Landing Zone-Version aktualisieren.

Wenn Sie Account Factory verwenden, um ein neues Konto zu erstellen oder ein bereits bestehendes Mitgliedskonto zu registrieren, oder wenn Sie Extend Governance auswählen, um Konten in einer bereits bestehenden Organisationseinheit zu registrieren, stellt AWS Control Tower seine Governance-Funktionen — einschließlich zentraler Protokollierung, Überwachung und Kontrollen — in den von Ihnen ausgewählten Regionen in den Konten bereit. Wenn Sie die Auswahl einer Region aufheben und die AWS Control Tower-Governance aus dieser Region entfernen, wird zwar diese Governance-Funktion entfernt, Ihre Benutzer werden jedoch nicht daran gehindert, AWS Ressourcen oder Workloads in diesen Regionen bereitzustellen.

AWS Control Tower funktioniert mit AWS Wichtige Managementsysteme

28. Juli 2021

(Optionales Update für die AWS Control Tower-Landezone)

AWS Control Tower bietet Ihnen die Möglichkeit, einen AWS Key Management Service (AWS KMS) -Schlüssel zu verwenden. Ein Schlüssel wird von Ihnen bereitgestellt und verwaltet, um die von AWS Control Tower bereitgestellten Dienste zu sichern AWS CloudTrail AWS Config, einschließlich und der zugehörigen Amazon S3-Daten. AWS Die KMS-Verschlüsselung ist eine höhere Verschlüsselungsstufe als die SSE-S3 Verschlüsselung, die AWS Control Tower standardmäßig verwendet.

Die Integration der AWS KMS-Unterstützung in den AWS Control Tower entspricht den AWS grundlegenden bewährten Sicherheitsmethoden, die eine zusätzliche Sicherheitsebene für Ihre vertraulichen Protokolldateien empfehlen. Sie sollten AWS KMS-verwaltete Schlüssel (SSE-KMS) für die Verschlüsselung im Ruhezustand verwenden. AWS KMS-Verschlüsselungsunterstützung ist verfügbar, wenn Sie eine neue Landing Zone einrichten oder wenn Sie Ihre bestehende AWS Control Tower-Landing Zone aktualisieren.

Um diese Funktion zu konfigurieren, können Sie bei der ersten Einrichtung der Landezone die KMS-Schlüsselkonfiguration auswählen. Sie können einen vorhandenen KMS-Schlüssel oder eine Schaltfläche auswählen, die Sie zur AWS KMS-Konsole weiterleitet, um einen neuen zu erstellen. Sie haben auch die Flexibilität, von der Standardverschlüsselung zu SSE-KMS oder zu einem anderen SSE-KMS Schlüssel zu wechseln.

Für eine bestehende AWS Control Tower-Landezone können Sie ein Update durchführen, um mit der Verwendung von AWS KMS-Schlüsseln zu beginnen.

Steuerung umbenannt, Funktionalität unverändert

26. Juli 2021

(Für die Landungszone des AWS Control Tower ist kein Update erforderlich)

AWS Control Tower überarbeitet derzeit bestimmte Kontrollnamen und Beschreibungen, um den politischen Absichten der Kontrolle besser Rechnung zu tragen. Die überarbeiteten Namen und Beschreibungen helfen Ihnen, intuitiver zu verstehen, wie Kontrollen die Richtlinien Ihrer Konten verkörpern. So haben wir zum Beispiel einen Teil der Namen der Detektivkontrollen von „Nicht zulassen“ in „Erkennen“ geändert, da die Detektivkontrolle selbst keine bestimmte Aktion stoppt, sondern lediglich Verstöße gegen die Richtlinien erkennt und über das Dashboard Warnmeldungen ausgibt.

Die Kontrollfunktionen, die Anleitung und die Implementierung bleiben unverändert. Lediglich die Namen und Beschreibungen der Kontrollen wurden überarbeitet.

Der AWS Control Tower scannt täglich SCPs, um nach Abweichungen zu suchen

11. Mai 2021

(Für die AWS Control Tower-Landezone ist kein Update erforderlich)

AWS Control Tower führt jetzt täglich automatische Scans Ihrer verwalteten SCPs durch, um sicherzustellen, dass die entsprechenden Kontrollen korrekt angewendet wurden und dass sie sich nicht geändert haben. Wenn bei einem Scan eine Abweichung festgestellt wird, erhalten Sie eine Benachrichtigung. AWS Control Tower sendet nur eine Benachrichtigung pro Drift-Problem. Wenn sich Ihre Landezone also bereits in einem Drift-Zustand befindet, erhalten Sie keine weiteren Benachrichtigungen, es sei denn, es wird ein neues Drift-Objekt gefunden.

Benutzerdefinierte Namen für Organisationseinheiten und Konten

16. April 2021

(Für die Landezone des AWS Control Tower ist kein Update erforderlich)

Mit AWS Control Tower können Sie jetzt die Benennung Ihrer Landezone anpassen. Sie können die Namen beibehalten, die AWS Control Tower für die Organisationseinheiten (OUs) und Hauptkonten empfiehlt, oder Sie können diese Namen während der ersten Einrichtung der Landezone ändern.

Die Standardnamen, die AWS Control Tower für die OUs und Kernkonten bereitstellt, entsprechen den Empfehlungen für bewährte Methoden für AWS mehrere Konten. Wenn Ihr Unternehmen jedoch bestimmte Benennungsrichtlinien hat oder Sie bereits eine Organisationseinheit oder ein Konto mit demselben empfohlenen Namen haben, können Sie mit der neuen Funktion zur Benennung von Organisationseinheiten und Konten flexibel auf diese Einschränkungen reagieren.

Unabhängig von dieser Workflow-Änderung während der Einrichtung wird die Organisationseinheit, die früher als Core-OU bekannt war, jetzt als Sicherheits-OU bezeichnet, und die OU, die früher als benutzerdefinierte OU bekannt war, wird jetzt Sandbox-OU genannt. Wir haben diese Änderung vorgenommen, um uns bei der Benennung besser an den allgemeinen Empfehlungen für AWS bewährte Verfahren auszurichten.

Neue Kunden werden diese neuen OU-Namen sehen. Bestandskunden werden weiterhin die ursprünglichen Namen dieser Organisationseinheiten angezeigt. Während wir unsere Dokumentation auf die neuen Namen aktualisieren, können einige Inkonsistenzen bei der Benennung von Organisationseinheiten auftreten.

Um von der AWS Managementkonsole aus mit AWS Control Tower zu beginnen, gehen Sie zur AWS Control Tower-Konsole und wählen Sie oben rechts die Option Landing Zone einrichten aus. Weitere Informationen finden Sie unter Planung Ihrer AWS Control Tower-Landezone.

AWS Control Tower-Landezone, Version 2.7

8. April 2021

(Für die Landing Zone des AWS Control Tower auf Version 2.7 ist ein Update erforderlich. Weitere Informationen finden Sie unterAktualisiere deine landing zone)

Mit AWS Control Tower Version 2.7 führt AWS Control Tower vier neue obligatorische präventive Protokollarchivierungskontrollen ein, mit denen Richtlinien ausschließlich für AWS Control Tower-Ressourcen implementiert werden. Wir haben die Leitlinien für vier bestehende Log-Archive-Kontrollen von verpflichtend zu fakultativ angepasst, da sie Richtlinien für Ressourcen außerhalb des AWS Control Towers festlegen. Diese Änderung und Erweiterung der Steuerung bietet die Möglichkeit, die Verwaltung von Protokollarchiven für Ressourcen innerhalb des AWS Control Tower von der Verwaltung von Ressourcen außerhalb des AWS Control Tower zu trennen.

Die vier geänderten Kontrollen können in Verbindung mit den neuen verbindlichen Kontrollen verwendet werden, um die Verwaltung einer breiteren Palette von AWS Protokollarchiven zu gewährleisten. In bestehenden AWS Control Tower-Umgebungen bleiben diese vier geänderten

Steuerelemente aus Gründen der Umgebungskonsistenz automatisch aktiviert. Diese optionalen Steuerelemente können jetzt jedoch deaktiviert werden. In neuen AWS Control Tower-Umgebungen müssen alle optionalen Steuerungen aktiviert werden. In bestehenden Umgebungen müssen die zuvor obligatorischen Kontrollen deaktiviert werden, bevor Amazon S3-Buckets, die nicht vom AWS Control Tower bereitgestellt werden, verschlüsselt werden.

Neue obligatorische Kontrollen:

- Verbieten Sie Änderungen an der Verschlüsselungskonfiguration für vom AWS Control Tower erstellte S3-Buckets im Protokollarchiv
- Verbieten Sie Änderungen an der Protokollierungskonfiguration für vom AWS Control Tower erstellte S3-Buckets im Protokollarchiv
- Verbieten Sie Änderungen an der Bucket-Richtlinie für vom AWS Control Tower erstellte S3-Buckets im Protokollarchiv
- Verbieten Sie Änderungen an der Lebenszykluskonfiguration für vom AWS Control Tower erstellte S3-Buckets im Protokollarchiv

Das Angebot wurde von Pflicht- auf Wahlfach geändert:

- Änderungen an der Verschlüsselungskonfiguration für alle Amazon S3-Buckets nicht zulassen [Bisher: Verschlüsselung im Ruhezustand für das Protokollarchiv aktivieren]
- Änderungen an der Protokollierungskonfiguration für alle Amazon S3-Buckets nicht zulassen [Bisher: Zugriffsprotokollierung für das Protokollarchiv aktivieren]
- Änderungen an der Bucket-Richtlinie für alle Amazon S3-Buckets verbieten [Bisher: Richtlinienänderungen am Log-Archiv verbieten]
- Änderungen an der Lebenszykluskonfiguration für alle Amazon S3-Buckets verbieten [Bisher: Festlegung einer Aufbewahrungsrichtlinie für das Protokollarchiv]

AWS Control Tower Version 2.7 beinhaltet Änderungen am AWS Control Tower Landing Zone Blueprint, die nach dem Upgrade auf 2.7 zu Inkompatibilität mit früheren Versionen führen können.

- Insbesondere AWS Control Tower Version 2.7 `BlockPublicAccess` wird automatisch für S3-Buckets aktiviert, die von AWS Control Tower bereitgestellt werden. Sie können diese Standardeinstellung deaktivieren, wenn Ihr Workload kontoübergreifenden Zugriff erfordert. Weitere Informationen darüber, was mit `BlockPublicaccess` enabled passiert, finden Sie unter Blockieren des öffentlichen Zugriffs auf Ihren Amazon S3-Speicher.

- AWS Control Tower Version 2.7 beinhaltet eine Anforderung für HTTPS. Alle Anfragen, die an von AWS Control Tower bereitgestellte S3-Buckets gesendet werden, müssen Secure Socket Layer (SSL) verwenden. Nur HTTPS-Anfragen dürfen weitergeleitet werden. Wenn Sie HTTP (ohne SSL) als Endpunkt zum Senden der Anfragen verwenden, erhalten Sie aufgrund dieser Änderung den Fehler „Zugriff verweigert“, der Ihren Workflow möglicherweise unterbrechen kann. Diese Änderung kann nach dem 2.7-Update für Ihre Landing Zone nicht mehr rückgängig gemacht werden.

  Wir empfehlen Ihnen, Ihre Anfragen so zu ändern, dass TLS anstelle von HTTP verwendet wird.

Drei neue AWS Regionen verfügbar

8. April 2021

(Update für die Landezone des AWS Control Tower erforderlich)

AWS Control Tower ist in drei weiteren AWS Regionen verfügbar: Asien-Pazifik (Tokio), Asien-Pazifik (Seoul) und Asien-Pazifik (Mumbai). Für die Ausweitung der Verwaltung auf diese Regionen ist ein Update der Landezone auf Version 2.7 erforderlich.

Deine Landezone wird nicht automatisch auf diese Regionen erweitert, wenn du das Update auf Version 2.7 durchführst. Du musst sie dir ansehen und in der Regionentabelle auswählen, damit sie aufgenommen werden können.

Nur ausgewählte Regionen verwalten

19. Februar 2021

(Für die Landezone des AWS Control Tower ist kein Update erforderlich)

Die Auswahl der AWS Control Tower-Region bietet eine bessere Möglichkeit, die geografische Präsenz Ihrer AWS Control Tower-Ressourcen zu verwalten. Um die Anzahl der Regionen zu erweitern, in denen Sie AWS Ressourcen oder Workloads hosten — aus Compliance-, regulatorischen, Kosten- oder anderen Gründen — können Sie jetzt die zusätzlichen Regionen auswählen, die Sie regeln möchten.

Die Regionsauswahl ist verfügbar, wenn Sie eine neue Landing Zone einrichten oder Ihre AWS Control Tower Landing Zone-Version aktualisieren. Wenn Sie Account Factory verwenden, um ein neues Konto zu erstellen oder ein bereits bestehendes Mitgliedskonto zu registrieren, oder wenn Sie Extend Governance verwenden, um Konten in einer bereits bestehenden Organisationseinheit zu

registrieren, stellt AWS Control Tower seine Governance-Funktionen zur zentralen Protokollierung, Überwachung und Steuerung in den von Ihnen ausgewählten Regionen in den Konten bereit. Weitere Informationen zur Auswahl von Regionen finden Sie unter. Konfigurieren Sie Ihre AWS Control Tower-Regionen

AWS Control Tower dehnt die Governance jetzt auf bestehende Organisationseinheiten in Ihrem Unternehmen aus AWS Organisationen

28. Januar 2021

(Für die Landezone des AWS Control Tower ist kein Update erforderlich)

Erweitern Sie die Governance von der AWS Control Tower-Konsole aus auf bestehende Organisationseinheiten (OUs) (die nicht im AWS Control Tower enthalten sind). Mit dieser Funktion können Sie OUs der obersten Ebene und inbegriffene Konten der AWS Control Tower-Verwaltung unterstellen. Informationen zur Ausweitung der Governance auf eine gesamte OU finden Sie unterRegistrieren Sie eine bestehende Organisationseinheit bei AWS Control Tower.

Wenn Sie eine OU registrieren, führt AWS Control Tower eine Reihe von Prüfungen durch, um sicherzustellen, dass die Governance und die Registrierung von Konten innerhalb der OU erfolgreich verlängert wurden. Weitere Informationen zu häufig auftretenden Problemen bei der Erstregistrierung einer OU finden Sie unter. Häufige Fehlerursachen bei der Registrierung oder erneuten Registrierung

Sie können auch die AWS Control Tower-Produktwebseite besuchen YouTube oder dieses Video über die ersten Schritte mit AWS Control Tower für ansehen AWS Organizations.

AWS Control Tower bietet massenweise Kontoaktualisierungen

28. Januar 2021

(Für die Landezone des AWS Control Tower ist kein Update erforderlich)

Mit der Funktion zur Massenaktualisierung können Sie jetzt alle Konten in einer registrierten AWS Organizations Organisationseinheit (OU) mit bis zu 300 Konten mit einem einzigen Klick über das AWS Control Tower-Dashboard aktualisieren. Dies ist besonders nützlich in Fällen, in denen Sie Ihre AWS Control Tower-Landing Zone aktualisieren und auch Ihre registrierten Konten aktualisieren müssen, um sie an die aktuelle Landing Zone-Version anzupassen.

Diese Funktion hilft Ihnen auch dabei, Ihre Konten auf dem neuesten Stand zu halten, wenn Sie Ihre AWS Control Tower-Landing Zone aktualisieren, um sie auf neue Regionen auszudehnen, oder wenn

Sie eine OU erneut registrieren möchten, um sicherzustellen, dass auf allen Konten in dieser OU die neuesten Kontrollen angewendet werden. Durch die Massenaktualisierung von Konten müssen Sie nicht mehr ein Konto nach dem anderen aktualisieren oder ein externes Skript verwenden, um die Aktualisierung für mehrere Konten durchzuführen.

Hinweise zum Aktualisieren einer Landing Zone finden Sie unterAktualisiere deine landing zone.

Hinweise zur Registrierung oder erneuten Registrierung einer Organisationseinheit finden Sie unterRegistrieren Sie eine bestehende Organisationseinheit bei AWS Control Tower.

Januar — Dezember 2020

Im Jahr 2020 veröffentlichte AWS Control Tower die folgenden Updates:

- Die AWS Control Tower-Konsole ist jetzt mit externen Geräten verknüpft AWS Konfigurationsregeln
- AWS Control Tower ist jetzt in weiteren Regionen verfügbar
- Aktualisierung der Leitplanke
- Die AWS Control Tower-Konsole zeigt mehr Details zu OUs und Konten
- Verwenden Sie AWS Control Tower, um ein neues Multikonto einzurichten AWS Umgebungen in AWS Organizations
- Anpassungen für die AWS Control Tower-Lösung
- Allgemeine Verfügbarkeit von AWS Control Tower Version 2.3
- Single-step Bereitstellung von Konten im AWS Control Tower
- Tool zur Außerbetriebnahme von AWS Control Tower
- Benachrichtigungen über Ereignisse im Lebenszyklus von AWS Control Tower

Die AWS Control Tower-Konsole ist jetzt mit externen Geräten verknüpft AWS Konfigurationsregeln

29. Dezember 2020

(Für die Landing Zone des AWS Control Tower auf Version 2.6 ist ein Update erforderlich. Weitere Informationen finden Sie unterAktualisiere deine landing zone)

AWS Control Tower enthält jetzt einen Aggregator auf Organisationsebene, der bei der Erkennung externer AWS Config-Regeln hilft. Auf diese Weise können Sie in der AWS Control Tower-Konsole

sehen, ob zusätzlich zu den von AWS Control Tower erstellten AWS Config-Regeln auch extern erstellte AWS Config-Regeln vorhanden sind. Der Aggregator ermöglicht es dem AWS Control Tower, externe Regeln zu erkennen und einen Link zur AWS Config-Konsole bereitzustellen, ohne dass der AWS Control Tower Zugriff auf nicht verwaltete Konten erhalten muss.

Mit dieser Funktion haben Sie jetzt eine konsolidierte Ansicht der auf Ihre Konten angewandten Ermittlungskontrollen, sodass Sie die Einhaltung der Vorschriften verfolgen und feststellen können, ob Sie zusätzliche Kontrollen für Ihr Konto benötigen. Weitere Informationen finden Sie unter So aggregiert AWS Control Tower AWS Config Regeln in nicht verwalteten Organisationseinheiten und Konten.

AWS Control Tower ist jetzt in weiteren Regionen verfügbar

18. November 2020

(Für die Landing Zone des AWS Control Tower auf Version 2.5 ist ein Update erforderlich. Weitere Informationen finden Sie unterAktualisiere deine landing zone)

AWS Control Tower ist jetzt in 5 weiteren AWS Regionen verfügbar:

- Region Asien-Pazifik (Singapur)
- Region Europa (Frankfurt)
- Region Europa (London)
- Region Europa (Stockholm)
- Region Kanada (Zentral)

Die Hinzufügung dieser 5 AWS Regionen ist die einzige Änderung, die für Version 2.5 von AWS Control Tower eingeführt wurde.

AWS Control Tower ist auch in den Regionen USA Ost (Nord-Virginia), USA Ost (Ohio), USA West (Oregon), Europa (Irland) und Asien-Pazifik (Sydney) verfügbar. Mit dieser Markteinführung ist der AWS Control Tower jetzt in 10 AWS Regionen verfügbar.

Dieses Landing Zone-Update umfasst alle aufgelisteten Regionen und kann nicht rückgängig gemacht werden. Nachdem Sie Ihre Landing Zone auf Version 2.5 aktualisiert haben, müssen Sie alle registrierten Konten manuell aktualisieren, damit AWS Control Tower in den 10 unterstützten AWS Regionen gilt. Weitere Informationen finden Sie unter Konfigurieren Sie Ihre AWS Control Tower-Regionen.

Aktualisierung der Leitplanke

8. Oktober 2020

(Für die Landezone des AWS Control Tower ist kein Update erforderlich)

Für die obligatorische Kontrolle wurde eine aktualisierte Version veröffentlicht`AWS-GR_IAM_ROLE_CHANGE_PROHIBITED`.

Diese Änderung der Steuerung ist erforderlich, da bei Konten, die automatisch bei AWS Control Tower registriert werden, die `AWSControlTowerExecution` Rolle aktiviert sein muss. Die vorherige Version des Steuerelements verhindert, dass diese Rolle erstellt wird.

Weitere Informationen finden Sie unter Verbieten von Änderungen an AWS IAM-Rollen, die von AWS Control Tower eingerichtet wurden, und CloudFormation im Referenzhandbuch zu AWS Control Tower Controls.

Die AWS Control Tower-Konsole zeigt mehr Details zu OUs und Konten

22. Juli 2020

(Für die Landezone des AWS Control Tower ist kein Update erforderlich)

Sie können Ihre Organisationen und Konten, die nicht bei AWS Control Tower registriert sind, zusammen mit Organisationen und Konten, die registriert sind, einsehen.

In der AWS Control Tower-Konsole können Sie weitere Details zu Ihren AWS Konten und Organisationseinheiten (OUs) einsehen. Auf der Seite Konten werden jetzt alle Konten in Ihrer Organisation aufgeführt, unabhängig von der Organisationseinheit oder dem Registrierungsstatus im AWS Control Tower. Sie können jetzt in allen Tabellen suchen, sortieren und filtern.

Verwenden Sie AWS Control Tower, um ein neues Multikonto einzurichten AWS Umgebungen in AWS Organizations

22. April 2020

(Für die Landezone des AWS Control Tower ist kein Update erforderlich)

AWS Organizations Kunden können jetzt AWS Control Tower verwenden, um neu erstellte Organisationseinheiten (OUs) und Konten zu verwalten, indem sie die folgenden neuen Funktionen nutzen:

- AWS Organizations Bestandskunden können jetzt in ihrem bestehenden Verwaltungskonto eine neue Landezone für neue Organisationseinheiten (OUs) einrichten. Mit AWS Control Tower Governance können Sie neue OUs in AWS Control Tower erstellen und in diesen OUs neue Konten erstellen.
- AWS Organizations Kunden können bestehende Konten mithilfe des Kontoregistrierungsprozesses oder mithilfe von Skripten registrieren.

AWS Control Tower bietet einen Orchestrierungsservice, der andere Dienste nutzt. AWS Es wurde für Organisationen mit mehreren Konten und Teams entwickelt, die nach der einfachsten Möglichkeit suchen, ihre neue oder bestehende AWS Umgebung mit mehreren Konten einzurichten und skalierbar zu verwalten. Bei einer Organisation, die vom AWS Control Tower geleitet wird, wissen Cloud-Administratoren, dass die Konten in der Organisation den festgelegten Richtlinien entsprechen. Entwickler profitieren davon, weil sie schnell neue AWS Konten einrichten können, ohne sich Gedanken über die Einhaltung der Vorschriften machen zu müssen.

Informationen zum Einrichten einer Landezone finden Sie unterPlanen Sie Ihre AWS Control Tower Tower-Landezone. Sie können auch die AWS Control Tower-Produktwebseite besuchen YouTube oder dieses Video über die ersten Schritte mit AWS Control Tower für ansehen AWS Organizations.

Zusätzlich zu dieser Änderung wurde die Funktion zur schnellen Kontobereitstellung im AWS Control Tower in Konto registrieren umbenannt. Sie ermöglicht jetzt die Registrierung vorhandener AWS Konten sowie die Erstellung neuer Konten. Weitere Informationen finden Sie unter Registrieren Sie ein vorhandenes Konto über die AWS Control Tower-Konsole.

Anpassungen für die AWS Control Tower-Lösung

17. März 2020

(Für die Landezone des AWS Control Tower ist kein Update erforderlich)

AWS Control Tower enthält jetzt eine neue Referenzimplementierung, mit der Sie ganz einfach benutzerdefinierte Vorlagen und Richtlinien auf Ihre AWS Control Tower-Landezone anwenden können.

Mit Anpassungen für AWS Control Tower können Sie CloudFormation Vorlagen verwenden, um neue Ressourcen für bestehende und neue Konten in Ihrer Organisation bereitzustellen. Zusätzlich zu den SCPs, die bereits von AWS Control Tower bereitgestellt werden, können Sie auf diese Konten auch benutzerdefinierte Service Control Policies (SCPs) anwenden. Anpassungen für die AWS Control

Tower-Pipeline lassen sich in die Ereignisse und Benachrichtigungen des AWS Control Tower-Lebenszyklus (Lebenszyklusereignisse im AWS Control Tower) integrieren, um sicherzustellen, dass die Ressourcenbereitstellungen mit Ihrer Landing Zone synchronisiert bleiben.

Die Bereitstellungsdokumentation für diese AWS Control Tower-Lösungsarchitektur ist auf der AWS Solutions-Webseite verfügbar.

Allgemeine Verfügbarkeit von AWS Control Tower Version 2.3

5. März 2020

(Für die Landezone des AWS Control Tower ist ein Update erforderlich. Weitere Informationen finden Sie unterAktualisiere deine landing zone.)

AWS Control Tower ist jetzt in der AWS Region Asien-Pazifik (Sydney) sowie in den Regionen USA Ost (Ohio), USA Ost (Nord-Virginia), USA West (Oregon) und Europa (Irland) verfügbar. Die Hinzufügung der Region Asien-Pazifik (Sydney) ist die einzige Änderung, die für Version 2.3 von AWS Control Tower eingeführt wurde.

Wenn Sie den AWS Control Tower noch nicht verwendet haben, können Sie ihn heute in jeder der unterstützten Regionen starten. Wenn Sie AWS Control Tower bereits verwenden und die Governance-Funktionen in Ihren Konten auf die Region Asien-Pazifik (Sydney) ausweiten möchten, gehen Sie in Ihrem AWS Control Tower-Dashboard zur Seite „Einstellungen“. Aktualisieren Sie von dort aus Ihre Landing Zone auf die neueste Version. Aktualisieren Sie dann Ihre Konten einzeln.

> **Note**
>
> Wenn Sie Ihre Landezone aktualisieren, werden Ihre Konten nicht automatisch aktualisiert. Wenn du mehr als ein paar Konten hast, können die erforderlichen Aktualisierungen zeitaufwändig sein. Aus diesem Grund empfehlen wir Ihnen, Ihre AWS Control Tower-Landezone nicht auf Regionen auszudehnen, in denen Ihre Workloads nicht ausgeführt werden müssen.

Informationen zum erwarteten Verhalten von Detective Controls als Ergebnis einer Bereitstellung in einer neuen Region finden Sie unter Konfigurieren Sie Ihre AWS Control Tower-Regionen.

Single-step Bereitstellung von Konten im AWS Control Tower

2. März 2020

(Für die Landezone des AWS Control Tower ist kein Update erforderlich)

AWS Control Tower unterstützt jetzt die Kontobereitstellung in einem Schritt über die AWS Control Tower-Konsole. Mit dieser Funktion können Sie neue Konten von der AWS Control Tower-Konsole aus bereitstellen.

Um das vereinfachte Formular zu verwenden, navigieren Sie in der AWS Control Tower-Konsole zu Account Factory und wählen Sie dann Quick Account Provisioning aus. AWS Control Tower weist dem bereitgestellten Konto und dem Single Sign-On-Benutzer (IAM Identity Center), der für das Konto erstellt wurde, dieselbe E-Mail-Adresse zu. Wenn Sie möchten, dass sich diese beiden E-Mail-Adressen unterscheiden, müssen Sie Ihr Konto über Service Catalog bereitstellen.

Aktualisieren Sie Konten, die Sie über die schnelle Kontobereitstellung mithilfe von Service Catalog und der AWS Control Tower Account Factory erstellen, genau wie Updates für jedes andere Konto.

> **Note**
>
> Im April 2020 wurde die Funktion zur schnellen Kontobereitstellung in Konto registrieren umbenannt. Im Juni 2022 wurde die Möglichkeit, Konten in der AWS Control Tower-Konsole zu erstellen und zu aktualisieren, von der Möglichkeit, Konten zu registrieren AWS , getrennt. Weitere Informationen finden Sie unter Registrieren Sie ein vorhandenes Konto über die AWS Control Tower-Konsole.

Tool zur Außerbetriebnahme von AWS Control Tower

28. Februar 2020

(Für die Landezone des AWS Control Tower ist kein Update erforderlich)

AWS Control Tower unterstützt jetzt ein automatisiertes Tool zur Außerbetriebnahme, das Sie bei der Bereinigung der vom AWS Control Tower zugewiesenen Ressourcen unterstützt. Wenn Sie nicht mehr beabsichtigen, AWS Control Tower für Ihr Unternehmen zu verwenden, oder wenn Sie eine größere Umverteilung Ihrer Unternehmensressourcen benötigen, sollten Sie möglicherweise die Ressourcen bereinigen, die Sie bei der ursprünglichen Einrichtung Ihrer Landing Zone erstellt haben.

Wenn Sie Ihre Landezone mithilfe eines größtenteils automatisierten Prozesses außer Betrieb nehmen möchten, wenden Sie sich an, AWS Support um Unterstützung bei den weiteren erforderlichen Schritten zu erhalten. Weitere Informationen zur Außerbetriebnahme finden Sie unter. Außerbetriebnahme einer AWS Control Tower Tower-Landezone

Benachrichtigungen über Ereignisse im Lebenszyklus von AWS Control Tower

22. Januar 2020

(Für die Landezone des AWS Control Tower ist kein Update erforderlich)

AWS Control Tower kündigt die Verfügbarkeit von Benachrichtigungen über Lebenszyklusereignisse an. Ein Lebenszyklusereignis markiert den Abschluss einer AWS Control Tower-Aktion, die den Status von Ressourcen wie Organisationseinheiten (OUs), Konten und Kontrollen, die vom AWS Control Tower erstellt und verwaltet werden, ändern kann. Ereignisse im Lebenszyklus werden als AWS CloudTrail Ereignisse aufgezeichnet und EventBridge als Ereignisse an Amazon übermittelt.

AWS Control Tower zeichnet Lebenszyklusereignisse nach Abschluss der folgenden Aktionen auf, die mit dem Service ausgeführt werden können: Erstellen oder Aktualisieren einer Landing Zone, Erstellen oder Löschen einer OU, Aktivieren oder Deaktivieren einer Kontrolle auf einer OU und Verwenden von Account Factory, um ein neues Konto zu erstellen oder ein Konto in eine andere OU zu verschieben.

AWS Control Tower verwendet mehrere AWS Dienste, um eine bewährte Umgebung mit mehreren Konten AWS aufzubauen und zu verwalten. Es kann mehrere Minuten dauern, bis eine AWS Control Tower-Aktion abgeschlossen ist. Sie können Lebenszyklusereignisse in den CloudTrail Protokollen verfolgen, um zu überprüfen, ob die ursprüngliche AWS Control Tower-Aktion erfolgreich abgeschlossen wurde. Sie können eine EventBridge Regel erstellen, um Sie zu benachrichtigen, wenn ein Lebenszyklusereignis CloudTrail aufgezeichnet wird, oder um automatisch den nächsten Schritt in Ihrem Automatisierungsworkflow auszulösen.

Juni — Dezember 2019

Vom 24. Juni bis 31. Dezember 2019 veröffentlichte AWS Control Tower die folgenden Updates:

- Allgemeine Verfügbarkeit von AWS Control Tower Version 2.2
- Neue optionale Steuerungen im AWS Control Tower
- Neue Detektivkontrollen im AWS Control Tower
- AWS Control Tower akzeptiert E-Mail-Adressen für gemeinsam genutzte Konten mit anderen Domänen als das Verwaltungskonto
- Allgemeine Verfügbarkeit von AWS Control Tower Version 2.1

Allgemeine Verfügbarkeit von AWS Control Tower Version 2.2

13. November 2019

(Für die Landezone des AWS Control Tower ist ein Update erforderlich. Weitere Informationen finden Sie unterAktualisiere deine landing zone.)

AWS Control Tower Version 2.2 bietet drei neue präventive Kontrollen, die eine Verschiebung der Konten verhindern:

- Verbieten Sie Änderungen an Amazon CloudWatch Logs-Protokollgruppen, die von AWS Control Tower eingerichtet wurden
- Verbieten Sie das Löschen von AWS Config Aggregationsberechtigungen, die von AWS Control Tower erstellt wurden
- Löschen des Protokollarchivs nicht zulassen

Eine Kontrolle ist eine allgemeine Regel, die die kontinuierliche Steuerung Ihrer gesamten AWS Umgebung gewährleistet. Wenn Sie Ihre AWS Control Tower-Landezone erstellen, entsprechen die Landezone und alle Organisationseinheiten (OUs), Konten und Ressourcen den Governance-Regeln, die durch die von Ihnen ausgewählten Kontrollen durchgesetzt werden. Wenn Sie und Ihre Organisationsmitglieder die Landezone nutzen, kann es zu (versehentlichen oder vorsätzlichen) Änderungen dieses Compliance-Status kommen. Die Erkennung von Abweichungen hilft Ihnen dabei, Ressourcen zu identifizieren, für die Änderungen oder Konfigurationsaktualisierungen erforderlich sind, um die Abweichung zu beheben. Weitere Informationen finden Sie unter Abweichungen im AWS Control Tower erkennen und beheben.

Neue optionale Steuerungen im AWS Control Tower

05. September 2019

(Für die AWS Control Tower-Landezone ist kein Update erforderlich)

Der AWS Control Tower umfasst jetzt die folgenden vier neuen Wahlsteuerungen:

- Löschen von Aktionen auf Amazon S3-Buckets ohne MFA nicht zulassen
- Verbieten Sie Änderungen an der Replikationskonfiguration für Amazon S3-Buckets
- Verbieten Sie Aktionen als Root-Benutzer
- Verbieten Sie die Erstellung von Zugriffsschlüsseln für den Root-Benutzer

Eine Kontrolle ist eine Regel auf hoher Ebene, die die kontinuierliche Steuerung Ihrer gesamten AWS Umgebung gewährleistet. Leitlinien ermöglichen es Ihnen, Ihre Richtlinienziele auszudrücken. Weitere Informationen finden Sie unter Über Steuerelemente im AWS Control Tower.

Neue Detektivkontrollen im AWS Control Tower

25. August 2019

(Für die Landezone des AWS Control Tower ist kein Update erforderlich)

Der AWS Control Tower umfasst jetzt die folgenden acht neuen Detektivkontrollen:

- Ermitteln Sie, ob die Versionierung für Amazon S3-Buckets aktiviert ist
- Ermitteln Sie, ob MFA für IAM-Benutzer der Konsole aktiviert ist AWS
- Stellen Sie fest, ob MFA für IAM-Benutzer aktiviert ist
- Ermitteln Sie, ob die Amazon EBS-Optimierung für Amazon EC2-Instances aktiviert ist
- Ermitteln Sie, ob Amazon EBS-Volumes an Amazon EC2-Instances angehängt sind
- Ermitteln Sie, ob der öffentliche Zugriff auf Amazon RDS-Datenbank-Instances aktiviert ist
- Ermitteln Sie, ob der öffentliche Zugriff auf Amazon RDS-Datenbank-Snapshots aktiviert ist
- Ermitteln Sie, ob die Speicherverschlüsselung für Amazon RDS-Datenbank-Instances aktiviert ist

Eine Kontrolle ist eine allgemeine Regel, die eine kontinuierliche Steuerung Ihrer gesamten AWS Umgebung gewährleistet. Eine detektivische Kontrolle erkennt Verstöße gegen die in Ihren Konten vorhandenen Ressourcen, wie z. B. Verstöße gegen Richtlinien, und informiert Sie über das Dashboard über Warnmeldungen. Weitere Informationen finden Sie unter Über Kontrollen im AWS Control Tower.

AWS Control Tower akzeptiert E-Mail-Adressen für gemeinsam genutzte Konten mit anderen Domänen als das Verwaltungskonto

01. August 2019

(Für die AWS Control Tower-Landezone ist kein Update erforderlich)

In AWS Control Tower können Sie jetzt E-Mail-Adressen für gemeinsam genutzte Konten (Log-Archiv und Audit-Mitglied) und untergeordnete Konten (mit Account Factory verkauft) angeben, deren

Domains sich von der E-Mail-Adresse des Verwaltungskontos unterscheiden. Diese Funktion ist nur verfügbar, wenn Sie eine neue Landezone erstellen und wenn Sie neue Kinderkonten einrichten.

Allgemeine Verfügbarkeit von AWS Control Tower Version 2.1

24. Juni 2019

(Für die Landezone des AWS Control Tower ist ein Update erforderlich. Weitere Informationen finden Sie unter Aktualisieren Sie Ihre Landing Zone.)

AWS Control Tower ist jetzt allgemein verfügbar und wird für den Produktionseinsatz unterstützt. AWS Control Tower richtet sich an Organisationen mit mehreren Konten und Teams, die nach der einfachsten Möglichkeit suchen, ihre neue AWS Umgebung mit mehreren Konten einzurichten und skalierbar zu verwalten. Mit AWS Control Tower können Sie sicherstellen, dass die Konten in Ihrer Organisation den festgelegten Richtlinien entsprechen. Endbenutzer in verteilten Teams können schnell neue AWS Konten einrichten.

Mithilfe von AWS Control Tower können Sie eine Landing Zone einrichten, die bewährte Methoden wie die Konfiguration einer Struktur mit mehreren Konten verwendet AWS Organizations, die Benutzeridentitäten und den Verbundzugriff mit verwaltet AWS IAM Identity Center, die Kontobereitstellung über Service Catalog ermöglicht und ein zentralisiertes Protokollarchiv mithilfe von und erstellt. AWS CloudTrail AWS Config

Für eine kontinuierliche Kontrolle können Sie vorkonfigurierte Kontrollen aktivieren, bei denen es sich um klar definierte Regeln für Sicherheit, Betrieb und Compliance handelt. Leitplanken verhindern den Einsatz von Ressourcen, die nicht den Richtlinien entsprechen, und überwachen die eingesetzten Ressourcen kontinuierlich auf Verstöße. Das AWS Control Tower-Dashboard bietet einen zentralen Überblick über eine AWS Umgebung, einschließlich der bereitgestellten Konten, der aktivierten Kontrollen und des Compliance-Status der Konten.

Sie können mit einem einzigen Klick in der AWS Control Tower-Konsole eine neue Umgebung mit mehreren Konten einrichten. Für die Nutzung von AWS Control Tower fallen keine zusätzlichen Gebühren oder Vorabverpflichtungen an. Sie zahlen nur für die AWS Services, die Sie für die Einrichtung einer Landezone und die Implementierung ausgewählter Kontrollen aktiviert haben.

Dokumentverlauf

- Letzte Aktualisierung der Dokumentation: 30. Dezember 2025

In der folgenden Tabelle werden wichtige Änderungen am AWS Control Tower Tower-Benutzerhandbuch beschrieben. Um Benachrichtigungen über Dokumentationsaktualisierungen zu erhalten, können Sie den RSS-Feed abonnieren.

Änderung	Beschreibung	Datum
Account Factory for Terraform (AFT) unterstützt reine Plananpassungsläufe	AFT unterstützt jetzt reine Plananpassungsläufe (schreibgeschützt) über die Eingabe in die Zustandsmaschine. `plan_only` `aft-invoke-customizations` AFT exportiert die Planausgabe standardmäßig in einen verschlüsselten Amazon S3 S3-Bucket in der Community Edition (Open Source) -Distribution. Der Export ist auf Terraform Cloud und Terraform Enterprise optional.	16. September 2026
Aktualisierung der verwalteten Richtlinie	Aktualisiert AWS ControlTowerServiceRolePolicy.	19. Mai 2026
Aktualisierung der verwalteten Richtlinie	Aktualisiert AWS ControlTowerAccountServiceRolePolicy.	19. Mai 2026
Aktualisierung der verwalteten Richtlinie	Aktualisiert AWS ControlTowerAccountServiceRolePolicy.	30. Dezember 2025

AWS Control Tower landing zone Version 4.0 mit spezieller Steuerungsumgebung	Die AWS Control Tower landing zone Version 4.0 ist jetzt mit optionalen Serviceintegrationen und einer speziellen Steuerungsumgebung verfügbar.	17. November 2025
AWS Control Tower umfasst weitere 279 AWS Config Kontrollen	Der Kontrollkatalog wurde um weitere 279 AWS Config Kontrollen aktualisiert.	14. November 2025
Aktualisierung der verwalteten Richtlinie	Aktualisiert AWS ControlTowerAccountServiceRolePolicy.	10. November 2025

Verwaltete Richtlinie aktualisiert	Aktualisiert AWS ControlTowerServiceRolePolicy, um die optionale AWS CloudTrail Integration von Landing Zone 4.0 zu unterstützen. Das Amazon CloudWatch Logs-Ressourcenmuster wurde von `aws-controltower/CloudTrailLogs:*` zu geändert, `aws-controltower/CloudTrailLogs*:*` um die Verwaltung von Protokollgruppen mit eindeutigen Suffixen zu ermöglichen. Dieses abwärtskompatible Update ermöglicht es Kunden, die AWS CloudTrail Integration mehrfach zu aktivieren und zu deaktivieren, wobei Protokollgruppen jedes Mal mit eindeutigen Suffixen neu erstellt werden, um Namenskonflikte zu vermeiden.	5. November 2025

Neue verwaltete Richtlinie	Dokumentation für AWS ControlTowerCloudTrailRolePolicyverwaltete Richtlinien hinzugefügt. Diese verwaltete Richtlinie ersetzt die zuvor von der verwendete Inline-Richtlinie AWS ControlTowerCloudTrailRole, sodass AWS die Richtlinie ohne Kundeneingriff aktualisiert werden kann.	5. November 2025
AWS Control Tower in der Region Asien-Pazifik (Neuseeland) verfügbar	AWS Control Tower ist in der Region Auckland, Neuseeland, verfügbar.	28. Oktober 2025
AWS Control Tower unterstützt die automatische Kontoregistrierung	Automatische Kontoregistrierung und Wechsel zwischen Organisationseinheiten.	15. Oktober 2025
Aktualisierung der verwalteten Richtlinie, neue verwaltete Richtlinie	Aktualisiert AWS ControlTowerServiceRolePolicyund neu hinzugefügt AWS ControlTowerIdentityCenterManagementPolicy.	14. Oktober 2025
AWS Control Tower aktualisiert die Python-Version	Aktualisierte Python-Versionen in AWS Control Tower Tower-Umgebungen	3. September 2025
AWS Control Tower unterstützt IPv6	AWS Control Tower bietet Unterstützung für IPv6-Endpunkte.	18. August 2025
Account Factory für Terraform Version 1.15.0	AFT Version 1.15.0 ist verfügbar.	28. Juli 2025

Aktualisierte Steuerelemente mit Nitro-Instanztypen	Acht proaktive Kontrollen wurden aktualisiert, um neue Instanztypen hinzuzufügen.	24. Juli 2025
AWS Control Tower im asiatisch-pazifischen Raum (Taipeh) verfügbar	AWS Control Tower bietet Unterstützung für den asiatisch-pazifischen Raum (Taipeh).	23. Juli 2025
AWS Control Tower unterstützt AWS PrivateLink	AWS Control Tower bietet Unterstützung für AWS PrivateLink.	30. Juni 2025
Service-linked AWS Config steuert	AWS Control Tower stellt servicebasierte Steuerungen bereit. AWS Config	12. Juni 2025
Verbesserte Metadaten. Zusätzliche Kontrollen, neue Frameworks	AWS Control Tower führt zusätzliche integrierte Kontrollen von ein AWS Config, mit erweiterten Metadaten für alle Kontrolle n im Control Catalog und Unterstützung für weitere Branchen-Frameworks.	12. Juni 2025
Ansicht der Steuerelemente aktiviert	AWS Control Tower bietet eine umfassende Konsolenansicht der aktivierten Steuerungen.	21. Mai 2025
AFT unterstützt neue Konfigurationen	AWS Control Tower AFT unterstützt drei zusätzliche optionale Konfigurationen bei der Bereitstellung.	13. Mai 2025
Verbesserte Baselines	AWS Control Tower meldet jetzt Basisabweichungen.	12. Mai 2025

AWS Control Tower ist in den Regionen AWS Asien-Pazifik (Thailand) und Mexiko (Mitte) verfügbar	Die folgenden Regionen sind verfügbar: Asien-Pazifik (Thailand) und Mexiko (Zentral).	9. Mai 2025
AWS Control Tower fügt 233 AWS Config Kontrollen hinzu	Neue Config-Steuerelemente, überarbeitete Metadatentabellen, Regionstabellen und Global Identifier-Seite hinzugefügt.	11. April 2025
AWS Control Tower aktualisiert eine serviceverknüpfte Rolle	Aktualisierungen für. `AWSControlTowerAccountServiceRolePolicy`	10. Dezember 2024
AWS Control Tower CfCT unterstützt GitHub	Eine neue Option für eine Konfigurationsquelle eines Drittanbieters.	9. Dezember 2024
Präventive Kontrollen von AWS Control Tower mit deklarativen Richtlinien	Eine neue Art von Richtlinie implementiert eine neue Art der präventiven Kontrolle.	01. Dezember 2024
AWS Control Tower lässt sich in AWS Backup integrieren	Sie können Pläne zur Sicherung Ihrer AWS Control Tower Tower-Ressourcen einrichten.	25. November 2024
AWS Control Tower integriert AWS Config Steuerungen	AWS Control Tower integriert ausgewählte AWS Config Steuerungen.	21. November 2024
AWS Control Tower verbessert das Hook-Management	AWS Control Tower verwaltet jetzt Hooks für proaktive Kontrollen.	20. November 2024

Abweichungen bei den Kontrollrichtlinien wurden gemeldet	AWS Control Tower meldet eine neue Art von Drift.	15. November 2024
AWS Control Tower führt Richtlinien zur verwalteten Ressourcenkontrolle ein	Eine neue Art von präventiven Kontrollen, implementiert mit RCPs.	15. November 2024
AWS Control Tower fügt ResetEnabledControl API hinzu	Eine neue API zur Verwaltung von Kontrollabweichungen.	14. November 2024
Aktualisierte `GetControl` API	Zwei neue Kontrollfelder für`GetControl` .	8. November 2024
AWS Control Tower AFT unterstützt Gitlab	Eine neue Option für eine Konfigurationsquelle eines Drittanbieters.	23. Oktober 2024
AWS Control Tower in der Region AWS Asien-Pazifik (Malaysia) verfügbar	Eine neue Region ist verfügbar , Malaysia (Kuala Lumpur).	21. Oktober 2024
AWS Control Tower unterstützt bis zu 1000 Konten pro Organisationseinheit	Eine Erhöhung des Limits für Konten pro OU.	30. August 2024
AWS Control Tower fügt eine Versionsauswahl für landing zone hinzu	Aktualisiere oder repariere deine landing zone, ohne zur neuesten Version zu wechseln, wenn du 3.1 oder neuer verwendest.	15. August 2024
GetControl und ListControls API-Operationen verfügbar	Zwei neue Control Catalog-Operationen helfen Ihnen dabei, mehr Informationen zu Steuerungen zu finden.	6. August 2024

AWS Control Tower unterstützt AFT und cFCT in Opt-in-Regionen	AFT und cFCT sind zusätzlich verfügbar. AWS-Regionen	18. Juli 2024
AWS Control Tower fügt die `ListLandingZoneOperations` API hinzu	Eine neue API, mit der Sie die letzten Operationen für Ihre landing zone abrufen können.	26. Juni 2024
AWS Control Tower unterstützt bis zu 100 gleichzeitige Kontrollvorgänge	Eine Erhöhung der Quote für gleichzeitige Kontrollvorgänge auf 100.	20. Mai 2024
AWS Control Tower in der Region AWS Calgary West (Kanada) verfügbar	AWS Control Tower ist in der Region Kanada West (Calgary) verfügbar.	3. Mai 2024
AWS Control Tower unterstützt Self-Service-Kontingentanpassungen	AWS Control Tower ist mit AWS Service Quotas in der Konsole integriert.	25. April 2024
Die Dokumentation für Kontrollen wurde in ein neues Handbuch verschoben	AWS Control Tower hat den Controls Reference Guide veröffentlicht.	21. April 2024
`EnabledControl` Ressourcen taggen in CloudFormation	AWS Control Tower unterstützt das Hinzufügen von Tags zu `EnabledControl` Ressourcen mithilfe von CloudFormation Vorlagen.	22. Februar 2024
Basis-APIs verfügbar	AWS Control Tower hat neue APIs für die programmg esteuerte Registrierung von Organisationseinheiten veröffentlicht.	14. Februar 2024

AWS-Control-Tower-Landezone, Version 3.3	Version 3.3 der AWS Control Tower Tower-Landezone verfügbar.	14. Dezember 2023
AWS Control Tower kündigt Kontrollen zur Unterstützung der digitalen Souveränität an	AWS Control Tower hat eine Reihe von Kontrollen veröffentlicht, um Kunden mit Anforderungen an die digitale Souveränität zu unterstützen.	27. November 2023
AWS Control Tower unterstützt Landingzone-APIs	AWS Control Tower unterstützt die Konfiguration und den Start von Landing Zones mithilfe neuer APIs.	26. November 2023
AWS Control Tower unterstützt Tagging-fähige Steuerelemente	AWS Control Tower unterstützt das Markieren aktivierter Steuerelemente in der Konsole und mit neuen APIs.	10. November 2023
AWS Control Tower im asiatisch-pazifischen Raum (Melbourne) verfügbar AWS-Region	Verfügbar in der Region Asien-Pazifik (Melbourne).	3. November 2023
Neue Kontroll-API verfügbar	AWS Control Tower hat eine neue Kontroll-API veröffentlicht.	14. Oktober 2023
AWS Control Tower führt neue Steuerungen ein	AWS Control Tower hat neue proaktive und detektive Kontrollen veröffentlicht.	05. Oktober 2023

AWS Control Tower meldet Abweichungen von der Deaktivierung des vertrauen swürdigen Zugriffs	AWS Control Tower benachric htigt Kunden, wenn Drift auftritt, wenn Kunden den vertrauenswürdigen Zugriff auf AWS Control Tower in AWS Organizations deaktivieren.	21. September 2023
AWS Control Tower ist in vier weiteren Varianten erhältlich AWS-Regionen	Erhältlich im asiatisch-pazifisc hen Raum (Hyderabad), Europa (Spanien und Zürich) und im Nahen Osten (VAE).	13. September 2023
AWS Control Tower in der Region Tel Aviv verfügbar	AWS Control Tower ist in der Region Tel Aviv, il-central-1, verfügbar.	28. August 2023
AWS Control Tower führt 28 neue proaktive Kontrollen ein	AWS Control Tower hat 28 neue proaktive Kontrollen veröffentlicht.	24. Juli 2023
AWS Control Tower lehnt zwei Steuerungen ab	AWS Control Tower wird mit Wirkung zum 18. August 2023 zwei Steuerelemente aus der Kontrollbibliothek entfernen.	18. Juli 2023
AWS Control Tower Tower-Landezone 3.2 verfügbar	Version 3.2 der AWS Control Tower landing zone ist verfügbar.	16. Juni 2023
AWS Control Tower verwaltet Konten auf der Grundlage von IDs	AWS Control Tower verfolgt die AWS Konto-ID und nicht die E-Mail-Adresse des Kontos.	14. Juni 2023

Zusätzliche Security Hub CSPM-Detektivkontrollen verfügbar	AWS Control Tower erweitert die Kontrollbibliothek um zehn neue Kontrollen für den Security Hub CSPM Service-Managed Standard: AWS Control Tower.	12. Juni 2023
AWS Control Tower veröffentlicht Tabellen mit Kontrollmetadaten	AWS Control Tower bietet jetzt Tabellen mit Kontrollmetadaten als Teil der veröffentlichten Dokumentation.	7. Juni 2023
Terraform-Unterstützung für Account Factory Customization	Single-region Unterstützung für Terraform-Open-Source-Blueprints in AFC.	6. Juni 2023
AWS IAM-Selbstmanagement für landing zone verfügbar	AWS Control Tower unterstützt Kunden jetzt bei der Auswahl ihres Identitätsanbieters für eine landing zone.	6. Juni 2023
Neue Rolle hinzugefügt	AWS Control Tower hat eine neue serviceverknüpfte Rolle und die zugehörige Richtlinie hinzugefügt. AWSServiceRoleForAWSControlTowerAWSControlTowerAccountServiceRolePolicy	01. Juni 2023
Update zur gemischten Unternehmensführung	Update zur Information von Kunden in Bezug auf gemischte Unternehmensführung	01. Juni 2023

Zusätzliche proaktive Kontrollen verfügbar	Neue proaktive Kontrollen unterstützen Sie bei der Verwaltung Ihrer Umgebung mit mehreren Konten und bei der Erfüllung bestimmter Kontrollziele.	19. Mai 2023
Sieben weitere Regionen verfügbar	AWS Control Tower ist jetzt in sieben weiteren Ländern verfügbar AWS-Regionen: Nordkalifornien (San Francisco), Asien-Pazifik (Hongkong, Jakarta und Osaka), Europa (Mailand), Naher Osten (Bahrain) und Afrika (Kapstadt).	19. April 2023
Wechseln Sie zu einer verwalteten Richtlinie	Wir haben das AWSControlTowerServiceRolePolicyso geändert, dass AWS Control Tower die`EnableRegion` ,`ListRegions` , `GetRegionOptStatus` APIs aufrufen kann, die vom AWS Account Management Service implementiert werden.	06. April 2023
Die Rückverfolgung von Anfragen zur Kontoanpassung ist allgemein verfügbar	AWS Control Tower unterstützt jetzt die Möglichkeit, Anfragen zur Kontoanpassung mithilfe des Account Factory for Terraform (AFT) -Workflows nachzuverfolgen.	16. Februar 2023

Aktualisierung der bewährten Methoden für IAM	Der Leitfaden wurde aktualisiert, um ihn an die Empfehlungen für bewährte IAM-Praktiken anzupassen. Weitere Informationen finden Sie unter Bewährte Sicherheitsmethoden in IAM.	15. Februar 2023
AWS Control Tower Tower-Landezone 3.1 verfügbar	Die AWS Control Tower landing zone 3.1 ist verfügbar.	9. Februar 2023
Proaktive Kontrollen sind allgemein verfügbar	Proaktive Kontrollen werden vom Vorschaustatus bis zur allgemeinen Verfügbarkeit eingeführt.	24. Januar 2023
Gleichzeitige Kontooperationen	AWS Control Tower unterstützt jetzt bis zu fünf (5) gleichzeitige Aktionen in Account Factory. Sie können bis zu fünf Konten gleichzeitig erstellen, aktualisieren oder registrieren.	16. Dezember 2022
Proaktive Kontrollen helfen bei der Bereitstellung von Ressourcen	AWS Control Tower unterstützt jetzt proaktive Kontrollen, die über CloudFormation Hooks implementiert werden.	28. November 2022
Anpassung des Kontos ab Werk verfügbar	AWS Control Tower unterstützt jetzt die Kontobereitstellung mit anpassbaren Kontovorlagen, sogenannten Blueprints, direkt von der AWS Control Tower Tower-Konsole aus.	28. November 2022

Der Compliance-Status ist für alle Regeln einsehbar AWS Config	AWS Control Tower zeigt jetzt den Compliance-Status aller AWS Config Regeln an, die in den bei AWS Control Tower registrierten Organisationseinheiten implementiert wurden.	18. November 2022
Änderung zu einer verwalteten Richtlinie	Wir haben das AWSControlTowerServiceRolePolicy so geändert, dass AWS Control Tower die `AWSControlTowerBlueprintAccess` Rolle übernehmen kann, die für Account Factory Factory-Anpassungen erforderlich ist.	28. Oktober 2022
APIs für Kontrollen, Ressourcen CloudFormation	AWS Control Tower unterstützt jetzt die Aktivierung und Deaktivierung von Kontrollen über eine Reihe von API-Aufrufen und eine neue CloudFormation Ressource.	01. September 2022
cFCT unterstützt das Löschen von Stack-Sets	CfCT unterstützt das Löschen von Stack-Sets, indem ein Parameter in der Manifestdatei gesetzt wird.	26. August 2022

Benutzerdefinierte Aufbewahrung von Protokollen	Sie können die Aufbewahrungsrichtlinie für Amazon S3 S3-Buckets, in denen Ihre AWS Control Tower CloudTrail Tower-Protokolle gespeichert werden, in Schritten von Tagen oder Jahren, bis zu einem Maximum von 15 Jahren, anpassen.	15. August 2022
Reparatur von Rollenabweichungen verfügbar	AWS Control Tower unterstützt die Reparatur von Rollenabweichungen, ohne dass die landing zone vollständig repariert werden muss.	11. August 2022
Version 3.0 verfügbar	AWS Control Tower landing zone Version 3.0 ändert sich von kontobasierten AWS CloudTrail Trails zu organisationsbasierten Trails und aktualisiert die verwaltete Richtlinie, um Trails auf Organisationsebene zu ermöglichen. Es ermöglicht Ihnen, AWS Config Informationen nur in Ihrer Heimatregion zu aggregieren. Version 3.0 enthält auch ein Update für die Option „Region Deny Control“ und zwei neue Detective Controls.	29. Juli 2022

Auf der Seite „Organisation“ werden Ansichten von Organisationseinheiten und Konten zusammengefasst	Die neue Organisationsseite in AWS Control Tower zeigt eine hierarchische Ansicht aller Organisationseinheiten (OUs) und Konten.	18. Juli 2022
Wechseln Sie zu einer verwalteten Richtlinie	Wir haben das AWSControlTowerServiceRolePolicyso geändert, dass Kunden über AWS CloudTrail Trails auf Organisationsebene verfügen können, um Logs zu aggregieren AWS CloudTrail .	20. Juni 2022
Einfachere Registrierung und Aktualisierung von Mitgliedskonten	AWS Control Tower bietet Ihnen jetzt die Möglichkeit, Mitgliedskonten einzeln von Ihrer landing zone aus zu registrieren und zu aktualisieren. Für jedes Konto wird angezeigt, wann es für ein Update verfügbar ist. Wir haben die Schaltfläche Konto registrieren vom Workflow Konto erstellen in Account Factory getrennt.	31. Mai 2022
AFT unterstützt die Anpassung für gemeinsam genutzte Konten	AWS Control Tower Account Factory for Terraform unterstützt jetzt die Anpassung für das AWS Control Tower Tower-Verwaltungskonto, das Protokollarchiv und die Auditkonten.	27. Mai 2022

Gleichzeitige Operationen für alle optionalen Kontrollen	Mit AWS Control Tower können Sie jetzt optionale vorbeugende Schutzmaß nahmen sowie detektive Kontrollen gleichzeitig anwenden und entfernen.	18. Mai 2022
Bestehende Sicherheits- und Protokollierungskonten	AWS Control Tower unterstüt zt jetzt die Möglichkeit, bestehende Sicherheits- und Protokollierungskonten mitzunehmen, anstatt bei der Einrichtung der landing zone neue zu erstellen.	16. Mai 2022
Version 2.9 verfügbar	AWS Control Tower landing zone Version 2.9 aktualisiert den Notification Forwarder Lambda, sodass er die Python-Laufzeit der Version 3.9 verwendet.	22. April 2022
Aktualisierte Unterstützung für AWS bewährte Methoden, Version 2.8 verfügbar	AWS Control Tower landing zone Version 2.8 bietet zusätzlichen Support, um sicherzustellen, dass Ihre Workloads und AWS Konten den AWS Best Practices entsprechen.	10. Februar 2022

Region verweigert Kontrolle	AWS Control Tower umfasst jetzt eine Steuerung, mit der Sie den Zugriff auf AWS Regionen einschränken können, um Compliance-Anforderungen und regulatorischen Bedenken Rechnung zu tragen.	30. November 2021
Kontrollen des Speicherorts der Daten	AWS Control Tower unterstützt jetzt Kontrollen, mit denen Sie die Datenresidenz mit detaillierter Kontrolle verwalten können.	30. November 2021
AWS Control Tower Account Factory für Terraform	AWS Control Tower unterstützt jetzt Terraform für die automatisierte Kontobereitstellung und -aktualisierung.	29. November 2021
Neues Lebenszyklus-Ereignis verfügbar	Das `PrecheckOrganizationalUnit` Ereignis protokolliert, ob Ressourcen, einschließlich Ressourcen in verschachtelten Organisationseinheiten, den Erfolg der Aufgabe „Steuerung erweitern“ verhindern.	18. November 2021
Verschachtelte Organisationseinheiten sind verfügbar	Mit AWS Control Tower kann Ihre landing zone jetzt verschachtelte OU-Strukturen enthalten.	16. November 2021

Parallelität mit detektivischer Kontrolle	AWS Control Tower Detective Controls unterstützen jetzt gleichzeitige Aktivierungs- und Deaktivierungsvorgänge.	5. November 2021
Zwei neue Regionen verfügbar	AWS Control Tower ist jetzt in zwei neuen AWS Regionen verfügbar: der Region Europa (Paris) und der Region Südamerika (São Paulo).	29. Juli 2021
Abwahl der Region	Sie können AWS Regionen abwählen, die Sie nicht mehr über AWS Control Tower verwalten möchten.	29. Juli 2021
KMS-Schlüssel verfügbar	Sie können optional von Ihnen verwaltete KMS-Schlüssel erstellen oder auswählen, um Ihre Daten und Ressourcen zu verschlüsseln.	28. Juli 2021
Wechseln Sie zu einer verwalteten Richtlinie	Wir haben die geändert, AWSControlTowerSer viceRolePolicysodass Kunden ihre eigenen KMS-Versc hlüsselungsschlüssel für AWS CloudTrail Protokolle verwenden können.	28. Juli 2021
Die Namen der Steuerele mente wurden geändert, die Funktionalität blieb unverände rt	Bestimmte Namen und Beschreibungen von Steuerele menten wurden aktualisiert, um die politischen Absichten der Kontrolle besser widerzusp iegeln, ohne dass sich die Funktionalität änderte.	26. Juli 2021

Automatisierte Scans verwalteter SCPs	AWS Control Tower führt täglich automatisierte Scans verwalteter SCPs durch, um zu überprüfen, ob Abweichungen vorliegen.	11. Mai 2021
Benutzerdefinierte Namen für Organisationseinheiten und Konten	Mit AWS Control Tower können Sie bei der Einrichtung der landing zone benutzerdefinierte Namen für wichtige Organisationseinheiten und Konten angeben, ohne dass es zu Abweichungen kommt.	16. April 2021
Die Außerbetriebnahme einer landing zone ist Self-Service	Mit AWS Control Tower können Sie jetzt eine landing zone außer Betrieb nehmen, ohne den AWS Support kontaktieren zu müssen. Die Außerbetriebnahme ist ein halbautomatisierter Prozess, der nicht rückgängig gemacht werden kann. Dies ist nicht dasselbe wie das manuelle Löschen aller AWS Control Tower Tower-Ressourcen.	9. April 2021
Drei weitere Regionen	AWS Control Tower ist jetzt in drei weiteren AWS Regionen verfügbar: Asien-Pazifik (Tokio), Asien-Pazifik (Seoul) und Asien-Pazifik (Mumbai).	8. April 2021

Neue Log Archive Controls, landing zone Version 2.7 verfügbar	Vier neue Log Archive-Kontrollen ermöglichen die Verwaltung von Protokollarchiven über AWS Control Tower-Ressourcen, getrennt von der Verwaltung von Ressourcen außerhalb von AWS Control Tower. Die Leitlinien für vier bestehende Kontrollen wurden von Pflicht- zu Wahlpflichtkontrollen geändert. Version 2.7 der AWS Control Tower landing zone beinhaltet eine HTTPS-Anforderung, die nach dem Update nicht rückgängig gemacht werden kann.	8. April 2021
Auswahl der Region	Die Auswahl der AWS Control Tower Tower-Region bietet eine bessere Möglichkeit, die geografische Präsenz Ihrer AWS Control Tower Tower-Ressourcen zu verwalten. Um die Anzahl der Regionen zu erhöhen, in denen Sie AWS Ressourcen oder Workloads hosten — aus Gründen der Einhaltung gesetzlicher Vorschriften, Kosten oder aus anderen Gründen — können Sie jetzt die zusätzlichen Regionen auswählen, die verwaltet werden sollen.	19. Februar 2021

Registrieren Sie eine Organisationseinheit und verwalten Sie alle ihre Konten gleichzeitig bei AWS Control Tower	AWS Control Tower bietet die Möglichkeit, eine Organisat ionseinheit zu registrieren. Auf diese Weise können mehrere Konten gleichzeitig verwaltet werden.	28. Januar 2021
Aktualisierungen mehrerer Konten in registrierten Organisationseinheiten	Sie können jetzt alle Konten in jeder registrierten AWS Organizations Organisat ionseinheit (OU) mit bis zu 300 Konten mit einem einzigen Klick über das AWS Control Tower Tower-Dashboard aktualisieren. Die Funktion zur Aktualisierung mehrerer Konten, auch als Bulk-Upda te bezeichnet, macht es überflüssig, jeweils ein Konto zu aktualisieren oder ein externes Skript zu verwenden , um die Aktualisierung für mehrere Konten gleichzeitig durchzuführen.	28. Januar 2021
Neue Rolle für die Aggregati on nicht verwalteter Organisat ionseinheiten und Konten	Eine neue Rolle hilft bei der Erkennung externer AWS Config Regeln, sodass AWS Control Tower keinen Zugriff auf nicht verwaltete Konten erhalten muss.	29. Dezember 2020

AWS Control Tower ist in weiteren AWS Regionen verfügbar.	AWS Control Tower ist jetzt für den Einsatz in den Regionen Asien-Pazifik (Singapur), Europa (Frankfurt), Europa (London), Europa (Stockholm) und Kanada (Zentral) verfügbar. Mit dieser Markteinführung ist AWS Control Tower jetzt in 10 AWS Regionen verfügbar. Dieses Landezone-Update umfasst alle aufgelisteten Regionen und kann nicht rückgängig gemacht werden. Nachdem Sie Ihre landing zone auf Version 2.5 aktualisiert haben, müssen Sie alle registrierten Konten für AWS Control Tower manuell aktualisieren, damit sie in den 10 unterstützten AWS Regionen verwaltet werden.	18. November 2020
Aktualisierung der Steuerung	Für die obligatorische Kontrolle wurde eine aktualisierte Version veröffentlicht `AWS-GR_IAM_ROLE_CHANGE_PROHIBITED` . Die aktualisierte Steuerung ermöglicht eine einfachere automatisierte Registrierung von Konten.	8. Oktober 2020

Die Seite mit verwandten Informationen ist jetzt für AWS Control Tower verfügbar	Die Seite mit den zugehörigen Informationen erleichtert das Auffinden häufiger Aufgaben, die nach der Einrichtung Ihrer AWS Control Tower Tower-Landingzone hilfreich sein können.	18. September 2020
Die AWS Control Tower Tower-Konsole zeigt mehr Details zu Organisationseinheiten und Konten.	In der AWS Control Tower Tower-Konsole können Sie weitere Informationen zu Ihren AWS Konten und Organisationseinheiten (OUs) einsehen. Auf der Seite „Konten“ werden jetzt alle Konten in Ihrer Organisation aufgeführt, unabhängig von der Organisationseinheit oder dem Registrierungsstatus in AWS Control Tower. Sie können jetzt in allen Tabellen suchen, sortieren und filtern.	22. Juli 2020

Mit AWS Control Tower können bestehende Organisationen eine landing zone einrichten.	Sie können jetzt in einer bestehenden Organisation eine landing zone für AWS Control Tower einrichten, um die Organisation unter Kontrolle zu bringen. Die Funktion zur schnellen Kontobereitstellung in AWS Control Tower wurde in Konto registrieren umbenannt und ermöglicht nun die Registrierung vorhandener AWS Konten sowie die Erstellung neuer Konten.	16. April 2020
AWS Control Tower ist jetzt im asiatisch-pazifischen Raum verfügbar	AWS Control Tower ist jetzt für den Einsatz in der AWS Region Asien-Pazifik (Sydney) verfügbar. Für diese Version sind manuelle Aktualisierungen der verkauften Konten erforderlich. Diese Aktualisierung sollte nur erfolgen, wenn Sie Workloads im asiatisch-pazifischen Raum (Sydney) ausführen möchten.	3. März 2020

Die Außerbetriebnahme einer AWS Control Tower Tower-Landezone ist möglich	AWS Der Support kann Ihnen dabei helfen, eine landing zone mithilfe eines weitgehend automatisierten Prozesses dauerhaft außer Betrieb zu nehmen, wodurch Ihre Organisation geschont wird, obwohl einige manuelle Aufräumarbeiten erforderlich sind.	27. Februar 2020
Schnelle Kontobereitstellung ist in AWS Control Tower verfügbar	Die schnelle Kontobereitstellung erleichtert das Starten neuer Mitgliedskonten bei aktueller Landing Zone mit der Funktion Enroll account (Konto anmelden).	20. Februar 2020
Lebenszyklusereignisse werden in AWS Control Tower verfolgt	Lifecycle-Ereignisse bieten zusätzliche Details für bestimmte AWS Control Tower Tower-Ereignisse, um die Workflow-Automatisierung zu vereinfachen.	12. Dezember 2019
Seiten mit Einstellungen und Aktivitäten sind für AWS Control Tower verfügbar	Die Einstellungs- und Aktivität enseiten erleichtern das Aktualisieren Ihrer Landing Zone und das Anzeigen protokollierter Ereignisse.	30. November 2019
Zusätzliche präventive Kontrollen sind für AWS Control Tower verfügbar.	Präventive Kontrollen in AWS Control Tower sorgen dafür, dass Ihr Unternehmen und Ihre Ressourcen auf Ihre Umgebung abgestimmt sind.	6. September 2019

Zusätzliche Detective Controls sind für AWS Control Tower verfügbar	Detective Controls in AWS Control Tower geben Aufschluss über den Status Ihrer Organisation und Ihrer Ressourcen.	27. August 2019
AWS Control Tower ist jetzt allgemein verfügbar	AWS Control Tower ist ein Service, der die einfachste Möglichkeit bietet, Ihre AWS Umgebung mit mehreren Konten in großem Umfang einzurichten und zu verwalten.	24. Juni 2019

AWS Glossar

Die neueste AWS Terminologie finden Sie im AWS Glossar in der AWS-Glossar Referenz.

Die vorliegende Übersetzung wurde maschinell erstellt. Im Falle eines Konflikts oder eines Widerspruchs zwischen dieser übersetzten Fassung und der englischen Fassung (einschließlich infolge von Verzögerungen bei der Übersetzung) ist die englische Fassung maßgeblich.