Benutzerhandbuch

AWS Control Tower

AWS Control Tower: Benutzerhandbuch

Table of Contents

Was ist AWS Control Tower? 1
Features 1
Wie AWS Control Tower mit anderen - AWS Services interagiert 2
Verwenden Sie AWS Control Tower zum ersten Mal? 3
So funktioniert’s 4
Struktur einer AWS-Kontrollturm-Landezone 4
Was passiert, wenn Sie eine landing zone einrichten 4
Was sind die gemeinsamen Konten? 5
Wie funktionieren Steuerungen 6
So funktioniert AWS Control Tower mit StackSets 7
Terminologie 9
Preisgestaltung 13
..... 13
Einrichtung 14
Melden Sie sich an für AWS 14
Melde dich an für eine AWS-Konto 14
Erstellen Sie einen Benutzer mit Administratorzugriff 15
..... 16
Nächster Schritt 16
Erste Schritte 17
Schnellstartanleitung 17
Prüfungen vor dem Start 19
Überlegungen für AWS IAM Identity Center (IAM Identity Center)-Kunden 20
Erste Schritte von der Konsole aus 21
Schritt 1: Erstellen Sie die E-Mail-Adressen für Ihr gemeinsames Konto 22
Erwartungen an die Konfiguration der landing zone 23
Schritt 2. Konfiguriere und starte deine landing zone 25
Schritt 3. Überprüfen und richten Sie die landing zone ein 33
Erste Schritte mit der Verwendung von APIs 34
Erwartungen an die Konfiguration der landing zone mit APIs 35
Schritt 1: Konfiguriere deine landing zone 36
Schritt 2: Starte deine landing zone 39
Identifizieren Sie Ihre landing zone 43
Aktualisiere deine landing zone 44

Setze die landing zone zurück, um Drift zu beheben 45
Machen Sie Ihre landing zone außer Betrieb 46
Beispiele: Einrichten einer Landing Zone von AWS Control Tower nur mit APIs 47
Starten einer landing zone mit AWS CloudFormation 55
Nächste Schritte 61
Einschränkungen und Kontingente 62
Einschränkungen in AWS Control Tower 62
Anfordern einer Kontingenterhöhung 64
Einschränkungen der Kontrolle 66
Regionen und Stapel setzen Grenzen 70
Regionale Unterschiede 71
Neu: Referenzhandbuch für AWS Control Tower Controls 72
Bewährte Methoden für Administratoren 73
Erläuterung des Zugriffs für Benutzer 73
Erläuterung des Ressourcenzugriffs 73
Erläuterung präventiver Kontrollen 74
Planen Ihrer Landing Zone 75
Vergleichen der Funktionalität 76
Starten von AWS Control Tower in einer vorhandenen Organisation 77
Starten von AWS Control Tower in einer neuen Organisation 79
Bewährte Methoden: Einrichten einer Landing Zone mit AWS mehreren Konten 79
Stimmen Sie sich mit der Anleitung für AWS mehrere Konten ab 80
Richtlinien für die Einrichtung einer gut strukturierten Umgebung 81
Beispiel für AWS Control Tower mit einer vollständigen Organisationseinheitsstruktur mit mehreren Konten 84
Informationen zum Root 85
Administrative Tipps für die Einrichtung der landing zone 85
Empfehlungen für die Einrichtung von Gruppen, Rollen und Richtlinien 87
Hinweise zu AWS Control Tower Tower-Ressourcen 88
Wann sollten Sie sich als Root-Benutzer anmelden 90
AWS Organizations Anleitung 91
Anleitung zum IAM Identity Center 93
Anleitung von Account Factory 95
Hinweise zum Abonnieren von SNS-Themen 95
Anleitung für KMS-Schlüssel 96
Richtlinien für KI-basierte Dienste 97

Verwaltung von Konfigurationsupdates 98
Informationen zu Aktualisierungen 100
Aktualisieren Ihrer Landing Zone 101
Manuelle Updates 101
Beheben Sie Abweichungen mit Reset und erneuter Registrierung 102
Konten mithilfe von Automatisierung bereitstellen und aktualisieren 103
Automatisieren Sie Aufgaben 105
AWS CloudShell und die AWS CLI 107
Abrufen von IAM-Berechtigungen für AWS CloudShell 108
Interaktion mit AWS Control Tower mithilfe von AWS CloudShell 108
AWS CloudFormation Ressourcen 112
AWS Control Tower und AWS CloudFormation Vorlagen 112
Erfahren Sie mehr über AWS CloudFormation 113
Passen Sie Ihre landing zone an 114
..... 114
Anpassen über die AWS Control Tower Tower-Konsole 114
Automatisieren Sie Anpassungen außerhalb der AWS Control Tower Tower-Konsole 116
Vorteile von Anpassungen für AWS Control Tower (cFCT) 116
Weitere CfCT-Beispiele 117
Übersicht über Anpassungen für AWS Control Tower (CfCT) 118
Architektur 118
Kosten 121
Komponentenservices 121
AWS CodeCommit 121
AWS CodePipeline 122
AWS Key Management Service 122
AWS Lambda 122
Amazon Simple Notification Service 122
Amazon Simple Storage Service 123
Amazon Simple Queue Service 123
AWS Step Functions 123
AWS Systems Manager Parameter Store 124
Überlegungen zur Bereitstellung 124
Vorbereiten der Bereitstellung 124
So aktualisieren Sie Anpassungen für AWS Control Tower 126
Vorlage und Quellcode 126

Quellcode ... 126
Bereitstellen von CfCT ... 127
Voraussetzungen ... 127
Schritte zur Bereitstellung ... 127
Schritt 1. Starten des -Stacks ... 127
Schritt 2. Erstellen eines benutzerdefinierten Pakets ... 132
Aktualisieren des Stacks ... 132
Löschen eines Stack-Sets ... 133
Einrichten von Amazon S3 als Konfigurationsquelle ... 135
Operationelle Metriken ... 136
Leitfaden zur cFcT-Anpassung ... 137
Überblick über die Code-Pipeline ... 138
Definieren Sie eine benutzerdefinierte Konfiguration ... 140
Stamm-OU ... 147
Verschachtelte Organisationseinheit ... 149
Erstellen Sie Ihre eigenen Anpassungen ... 150
Manifeste Versionsupgrades ... 158
Netzwerk ... 161
VPCs und AWS Regionen in AWS Control Tower ... 161
Überblick über AWS Control Tower und VPCs ... 162
... 162
CIDR und Peering für VPC und AWS Control Tower ... 163
Rollen und Berechtigungen ... 166
Rollen und Konten ... 167
Rollen und Kontoerstellung ... 167
AWSControlTowerExecution Rolle ... 168
Optionale Bedingungen für Ihre Rolle, Vertrauensbeziehungen ... 169
So aggregiert AWS Control Tower AWS Config Regeln in nicht verwalteten Organisationseinheiten und Konten ... 172
Programmgesteuerte Rollen und Vertrauensbeziehungen für das AWS Control Tower Tower-Auditkonto ... 174
Automatisierte Kontobereitstellung mit IAM-Rollen ... 178
Ressourcen verwalten ... 180
Regionen konfigurieren ... 181
Konfigurieren Sie Ihre AWS Control Tower Tower-Regionen ... 182
Vermeiden Sie gemischte Verwaltungsstrukturen bei der Konfiguration von Regionen ... 184

Über Opt-in-Regionen 186
Konfigurieren Sie die Option „Region Deny Control“ 189
Überlegungen zur Region Deny Control auf OU-Ebene 191
Konten 192
Methoden der Bereitstellung 192
Was passiert, wenn AWS Control Tower ein Konto erstellt 194
Erforderliche Berechtigungen 194
..... 195
Informationen zu -Konten 195
Überlegungen zur Mitnahme vorhandener Sicherheits- oder Protokollkonten 196
Sehen Sie sich Ihre Konten an 196
Ressourcen für gemeinsam genutzte Konten 197
Über die gemeinsamen Konten 208
Über Mitgliedskonten 211
Registriere ein vorhandenes AWS-Konto 211
Was passiert bei der Kontoregistrierung 212
Registrierung vorhandener Konten bei VPCs 214
Voraussetzungen für die Registrierung 214
Registriere ein Konto 215
Was ist, wenn das Konto die Voraussetzungen nicht erfüllt? 219
Beispiel für AWS Config CLI-Befehle für den Ressourcenstatus 221
Fügen Sie die erforderliche IAM-Rolle manuell zu einer vorhandenen hinzu AWS-Konto und registrieren Sie sie 222
Automatisierte Registrierung von Konten AWS Organizations 224
Registrieren von Konten mit vorhandenen AWS Config Ressourcen 225
Schritt 1: Wenden Sie sich mit einem Ticket an den Kundensupport, um das Konto zur Zulassungsliste von AWS Control Tower hinzuzufügen 228
Schritt 2: Erstellen einer neuen IAM-Rolle im Mitgliedskonto 228
Schritt 3: Identifizieren der AWS Regionen mit bereits vorhandenen Ressourcen 229
Schritt 4: Identifizieren der AWS Regionen ohne AWS Config Ressourcen 229
Schritt 5: Ändern der vorhandenen Ressourcen in jeder AWS Region 229
Schritt 5a. AWS Config Recorder-Ressourcen 230
Schritt 5b. Ändern der Ressourcen des AWS Config Übermittlungskanals 231
Schritt 5c. Ändern von Ressourcen für die AWS Config Aggregationsautorisierung 231
Schritt 6: Erstellen von Ressourcen, in denen sie nicht vorhanden sind, in Regionen, die von AWS Control Tower verwaltet werden 232

Schritt 7: Registrieren der Organisationseinheit bei AWS Control Tower 233
Account Factory 234
Berechtigungen 234
Erstellen Sie ein Konto und stellen Sie es bereit 234
Überlegungen zum Konto 236
Konten aktualisieren und verschieben 236
Ändern Sie die E-Mail-Adresse eines registrierten Kontos 239
Ändern Sie den Namen eines registrierten Kontos 240
Amazon VPC-Einstellungen konfigurieren 240
Verwaltung eines Kontos aufheben 242
Schließen Sie ein Konto 244
Ressourcen von Account Factory 245
Anpassung Account Factory (AFC) 247
Für die Anpassung eingerichtet 250
Erstellen Sie ein benutzerdefiniertes Konto anhand eines Blueprints 256
Registrieren Sie Konten und passen Sie sie an 258
Einen Blueprint zu einem AWS Control Tower Tower-Konto hinzufügen 258
Aktualisieren Sie einen Blueprint 259
Entfernen Sie einen Blueprint aus einem Konto 260
Blueprints von Partnern 260
Überlegungen zu Account Factory Factory-Anpassungen (AFC) 260
Im Falle eines Blueprint-Fehlers 261
Anpassen Ihres Richtliniendokuments für AFC-Blueprints auf der Grundlage von CloudFormation 263
Zusätzliche Berechtigungen sind für die Erstellung eines Terraform-basierten Service Catalog-Produkts erforderlich 264
AWS Control Tower Account Factory für Terraform (AFT) 265
Voraussetzungen 266
Richten Sie ein neues Konto ein 266
Mehrere Kontoanfragen 268
Aktualisieren Sie ein bestehendes Konto 268
Stellen Sie AFT bereit 269
Überblick über AFT 274
Unterstützte Versionen 278
Aktivieren von Feature-Optionen 282
Ressourcen für AFT 285

Erforderliche Rollen 289
Komponentenservices 292
Pipeline zur Bereitstellung von AFT-Konten 294
Anpassungen des Kontos 297
Alternatives VCS 304
Datenschutz 306
Entfernen eines Kontos 307
Operationelle Metriken 309
Anleitung zur Fehlerbehebung 310
Abweichungen 315
Drift erkennen 315
Behebung von Abweichungen 317
Überlegungen zu Drift- und SCP-Scans 317
Arten von Abweichungen, die sofort behoben werden müssen 319
Reparierbare Änderungen an Ressourcen 320
Abweichungen und Bereitstellung neuer Konten 320
Arten von Governance-Abweichungen 321
Moved Member Account (Mitgliedskonto verschoben) 322
Removed Member Account (Mitgliedskonto entfernt) 324
Unplanned Update to Managed SCP (Außerplanmäßige Aktualisierung einer verwalteten SCP) 325
SCP Attached to Managed OU (SCP ist einer verwalteten Organisationseinheit zugeordnet) 326
SCP Detached from Managed OU (SCP von verwalteter Organisationseinheit getrennt) 327
SCP Attached to Member Account (SCP ist einem Mitgliedskonto zugeordnet) 328
Die grundlegende Organisationseinheit wurde gelöscht 329
Security Hub steuert Drift 330
Vertrauenswürdiger Zugriff deaktiviert 331
Wenn Sie Ressourcen außerhalb von AWS Control Tower verwalten 332
Verweis auf Ressourcen außerhalb von AWS Control Tower 333
Externes Ändern von AWS Control Tower Tower-Ressourcennamen 333
Löschen der Sicherheits-Organisationseinheit 334
Ein Konto aus der Sicherheits-OU entfernen 335
Externe Änderungen, die automatisch aktualisiert werden 338
Organisationen 340
Video-Anleitung 341

... 341
Erweitern der Governance auf eine bestehende Organisation ... 341
Video: Aktivieren einer Landing Zone in vorhandenen AWS Organizations ... 343
Überlegungen zu IAM Identity Center und bestehenden Organisationen ... 343
Zugriff auf andere - AWS Services ... 343
Verschachtelte Organisationseinheiten ... 343
Video-Anleitung ... 344
Erweitern Sie von einer flachen OU-Struktur zu einer verschachtelten OU-Struktur ... 344
Vorabprüfungen für die Registrierung verschachtelter Organisationseinheiten ... 345
Verschachtelte Organisationseinheiten und Rollen ... 345
Was passiert bei der Registrierung und erneuten Registrierung von verschachtelten Organisationseinheiten und Konten ... 346
Überlegungen zur Registrierung verschachtelter Organisationseinheiten ... 346
Einschränkungen verschachtelter Organisationseinheiten ... 347
Verschachtelte Organisationseinheiten und Konformität ... 347
Verschachtelte Organisationseinheiten und Drift ... 348
Verschachtelte Organisationseinheiten und Kontrollen ... 348
Verschachtelte Organisationseinheiten und das Stammverzeichnis ... 350
Registrieren Sie eine Organisationseinheit, um mehrere Konten zu registrieren ... 350
Registrieren Sie eine bestehende Organisationseinheit ... 352
Erstellen Sie eine neue Organisationseinheit ... 354
Häufige Ursachen für Fehler bei der Registrierung oder Neuregistrierung ... 355
Organisationen aktualisieren ... 357
Wann sollten OUs und Konten aktualisiert werden ... 358
Aktualisieren mehrerer Konten in einer Organisationseinheit ... 358
Was passiert während der Neuregistrierung? ... 358
Aktualisieren eines einzelnen Kontos ... 359
Integrierte Services ... 361
AWS CloudFormation ... 361
CloudTrail ... 362
CloudWatch ... 362
AWS Config ... 362
AWS Identity and Access Management ... 363
AWS Key Management Service ... 363
AWS Lambda ... 364
AWS Organizations ... 364

Überlegungen ... 365
Amazon S3 ... 365
Security Hub ... 365
AWS Service Catalog ... 366
Übergang zum externen Produkttyp ... 366
Amazon SNS ... 368
Step Functions ... 368
Identity and Access Management ... 369
Authentifizierung ... 369
Zugriffskontrolle ... 372
IAM Identity Center und AWS Control Tower ... 372
... 372
Benutzergruppen, Rollen und Berechtigungssätze ... 373
Wissenswertes über IAM Identity Center-Konten und AWS Control Tower ... 374
IAM Identity Center-Gruppen für AWS Control Tower ... 375
Überblick über die Verwaltung des Ressourcenzugriffs mit IAM ... 379
Ressourcen und Betriebsabläufe von AWS Control Tower ... 379
Über den Besitz von Ressourcen ... 380
Zugriff auf Ressourcen verwalten ... 380
Geben Sie die Richtlinienelemente an: Aktionen, Auswirkungen und Prinzipien ... 391
Angeben von Bedingungen in einer Richtlinie ... 392
Vermeiden Sie Angriffe mit verwirrten Stellvertretern ... 392
IAM-Richtlinien für AWS Control Tower ... 393
Für die Nutzung der AWS Control Tower Tower-Konsole sind Berechtigungen erforderlich ... 393
AWS ControlTowerAdmin Rolle ... 394
AWS ControlTowerServiceRolePolicy ... 395
AWS ControlTowerStackSetRole ... 400
AWS ControlTowerCloudTrailRole ... 401
AWSControlTowerBlueprintAccess Anforderungen an die Rolle ... 402
AWSServiceRoleForAWSControlTower ... 403
AWSControlTowerAccountServiceRolePolicy ... 404
Verwaltete Richtlinien für AWS Control Tower ... 406
Sicherheit ... 411
Datenschutz ... 411
Verschlüsselung im Ruhezustand ... 413
Verschlüsselung während der Übertragung ... 413

Einschränken des Zugriffs auf Inhalte ... 413
Compliance-Validierung ... 414
Ausfallsicherheit ... 415
Sicherheit der Infrastruktur ... 415
Protokollierung und Überwachung ... 417
Über die Anmeldung bei AWS Control Tower ... 418
S3-Bucket-Richtlinie ... 419
Überblick über die Überwachung ... 421
Protokollieren von AWS Control Tower-Aktionen mit AWS CloudTrail ... 422
AWS Control Tower-Informationen in CloudTrail ... 422
Beispiel: AWS Control Tower-Protokolldateieinträge ... 425
Überwachen von Ressourcenänderungen mit AWS Config ... 426
Verwalten von Config-Kosten ... 427
Anzeigen der AWS Config Recorder-Daten für registrierte Konten ... 429
Fehlerbehebung AWS Config in AWS Control Tower ... 429
Ereignisse im Lebenszyklus ... 431
`CreateManagedAccount` ... 434
`UpdateManagedAccount` ... 436
`EnableGuardrail` ... 437
`DisableGuardrail` ... 438
`SetupLandingZone` ... 440
`UpdateLandingZone` ... 441
`RegisterOrganizationalUnit` ... 443
`DeregisterOrganizationalUnit` ... 445
`PrecheckOrganizationalUnit` ... 446
Benutzerbenachrichtigungen ... 448
Anleitungen ... 451
Walkthrough: Von ALZ zu AWS Control Tower wechseln ... 451
Walkthrough: Automatisieren der Kontobereitstellung in AWS Control Tower über Service-Catalog-APIs ... 452
Beispiel für eine Bereitstellungseingabe für die Service-Catalog-API ... 454
Video-Anleitung ... 455
Exemplarische Vorgehensweise: Konfiguration von AWS Control Tower ohne VPC ... 456
Löschen Sie die AWS Control Tower VPC ... 456
Erstellen Sie ein Konto in AWS Control Tower ohne VPC ... 457

Walkthrough: Einrichten von Sicherheitsgruppen in AWS Control Tower mit AWS Firewall Manager ... 459
Einrichten von Sicherheitsgruppen mit AWS Firewall Manager ... 459
Exemplarische Vorgehensweise: Außerbetriebnahme einer AWS Control Tower Tower-Landezone ... 459
Überblick über den Außerbetriebnahmeprozess ... 461
Ressourcen, die bei der Außerbetriebnahme nicht entfernt wurden ... 462
Wie man eine landing zone außer Betrieb nimmt ... 472
... 474
Einrichtung nach der Außerbetriebnahme einer landing zone ... 475
Fehlerbehebung ... 477
Start der Landing Zone fehlgeschlagen ... 477
Fehler „Landezone ist nicht aktuell“ ... 478
New Account Provisioning Failed (Bereitstellung eines neuen Kontos fehlgeschlagen) ... 478
Ein bestehendes Konto konnte nicht angemeldet werden ... 479
Ein Account Factory-Konto konnte nicht aktualisiert werden ... 480
Die Landing Zone konnte nicht aktualisiert werden ... 482
Fehler: Erwähnter Fehler AWS Config ... 483
Fehler: Keine Startpfade gefunden ... 485
Fehler „Unzureichende Berechtigungen“ erhalten ... 486
Detektivkontrollen wirken sich nicht auf Konten aus ... 486
Der Fehler „Rate überschritten“ wurde von der AWS Organizations API zurückgegeben ... 487
Fehler beim Verschieben eines Account Factory Factory-Kontos direkt von einer AWS Control Tower Tower-Landezone in eine andere AWS Control Tower Tower-Landezone ... 488
AWS Support ... 490
Baselines ... 491
Teilweise Registrierung von Konten ... 493
Unterschiede im Betrieb zwischen der AWS Control Tower Tower-Konsole und APIs für Baselines ... 494
Baselines und Standardeinstellungen für die Versionierung ... 494
AWSControlTowerBaseline Tabelle ... 495
Beispiele: Registrieren Sie eine AWS Control Tower Tower-Organisationseinheit nur mit APIs ... 499
Baseline-API-Beispiele ... 501
`DisableBaseline` ... 501
`EnableBaseline` ... 502

GetBaseline ... 504
GetBaselineOperation ... 504
GetEnabledBaseline ... 505
ListBaselines ... 506
ListEnabledBaselines ... 507
ResetEnabledBaseline ... 509
UpdateEnabledBaseline ... 510
Ähnliche Informationen ... 512
Tutorials und Übungen ... 512
Netzwerk ... 161
Sicherheit, Identität und Protokollierung ... 513
Bereitstellung von Ressourcen und Verwaltung von Workloads ... 514
Arbeit mit bestehenden Organisationen und Konten ... 514
Automatisierung und Integration ... 514
Workloads migrieren ... 515
Zugehörige AWS-Services ... 515
AWS Marketplace Lösungen ... 516
Versionshinweise ... 517
Januar 2024 - Heute ... 517
AWS Control Tower unterstützt bis zu 100 gleichzeitige Kontrollvorgänge ... 518
AWS Control Tower in AWS Kanada West (Calgary) verfügbar ... 518
AWS Control Tower unterstützt Self-Service-Kontingentanpassungen ... 520
AWS Control Tower veröffentlicht den Controls Reference Guide ... 520
AWS Control Tower aktualisiert und benennt zwei proaktive Kontrollen um ... 520
Veraltete Steuerelemente sind nicht mehr verfügbar ... 521
AWS Control Tower unterstützt das Taggen von EnabledControl Ressourcen in AWS CloudFormation ... 521
AWS Control Tower unterstützt APIs für die Registrierung und Konfiguration von Organisationseinheiten mit Baselines ... 522
Januar 2023 — Heute ... 523
Übergang zum neuen AWS Service Catalog externen Produkttyp (Phase 3) ... 525
AWS-Control-Tower-Landezone, Version 3.3 ... 525
Umstellung auf einen neuen AWS Service Catalog externen Produkttyp (Phase 2) ... 526
AWS Control Tower kündigt Kontrollen zur Unterstützung der digitalen Souveränität an ... 526
AWS Control Tower unterstützt Landingzone-APIs ... 532
AWS Control Tower unterstützt Tagging für aktivierte Kontrollen ... 533

AWS Control Tower in der Region Asien-Pazifik (Melbourne) verfügbar 534
Umstellung auf den neuen AWS Service Catalog externen Produkttyp (Phase 1) 534
Neue Kontroll-API verfügbar 535
AWS Control Tower fügt zusätzliche Kontrollen hinzu 536
Es wurde ein neuer Drift-Typ gemeldet: Vertrauenswürdiger Zugriff deaktiviert 539
Vier weitere AWS-Regionen 539
AWS Control Tower in der Region Tel Aviv verfügbar 539
AWS Control Tower führt 28 neue proaktive Kontrollen ein 540
AWS Control Tower lehnt zwei Kontrollen ab 542
AWS-Control-Tower-Landezone, Version 3.2 543
AWS Control Tower verwaltet Konten auf der Grundlage von IDs 545
Zusätzliche Security Hub Hub-Detektivkontrollen sind in der AWS Control Tower Tower-Steuerungsbibliothek verfügbar 545
AWS Control Tower veröffentlicht Tabellen mit Kontrollmetadaten 546
Terraform-Unterstützung für Account Factory Customization 546
AWS IAM Identity Center-Selbstmanagement für die landing zone verfügbar 547
AWS Control Tower befasst sich mit gemischter Governance für Organisationseinheiten 548
Zusätzliche proaktive Kontrollen verfügbar 548
Aktualisierte proaktive Amazon EC2 EC2-Kontrollen 551
AWS-Regionen Sieben weitere verfügbar 551
Rückverfolgung von Anfragen zur Kontoanpassung von Account Factory for Terraform (AFT) 552
AWS-Control-Tower-Landezone, Version 3.1 553
Proaktive Kontrollen sind allgemein verfügbar 554
Januar — Dezember 2022 555
Gleichzeitige Kontooperationen 555
Anpassung Account Factory (AFC) 556
Umfassende Kontrollen helfen bei der Bereitstellung und AWS Verwaltung von Ressourcen 556
Der Compliance-Status ist für alle AWS Config Regeln einsehbar 557
API für Kontrollen und eine neue AWS CloudFormation Ressource 558
cFCT unterstützt das Löschen von Stack-Sets 559
Benutzerdefinierte Aufbewahrung von Protokollen 559
Reparatur von Role Drift verfügbar 560
AWS-Control-Tower-Landezone, Version 3.0 560

Auf der Organisationsseite werden Ansichten von Organisationseinheiten und Konten zusammengefasst ... 564
Einfachere Registrierung und Aktualisierung für einzelne Mitgliedskonten ... 564
AFT unterstützt automatisierte Anpassungen für gemeinsam genutzte AWS Control Tower Tower-Konten ... 565
Gleichzeitige Operationen für alle optionalen Steuerelemente ... 566
Bestehende Sicherheits- und Protokollierungskonten ... 567
AWS-Control-Tower-Landezone, Version 2.9 ... 568
AWS-Control-Tower-Landezone, Version 2.8 ... 568
Januar bis Dezember 2021 ... 569
Region verweigert Funktionen ... 570
Funktionen zur Datenresidenz ... 570
AWS Control Tower führt die Bereitstellung und Anpassung von Terraform-Konten ein ... 571
Neues Lebenszyklus-Ereignis verfügbar ... 572
AWS Control Tower ermöglicht verschachtelte Organisationseinheiten ... 572
Parallelität mit detektivischer Kontrolle ... 573
Zwei neue Regionen verfügbar ... 574
Abwahl der Region ... 574
AWS Control Tower arbeitet mit AWS Schlüsselverwaltungssystemen ... 575
Steuerung umbenannt, Funktionalität unverändert ... 576
AWS Control Tower scannt SCPs täglich, um zu prüfen, ob Abweichungen vorliegen ... 576
Benutzerdefinierte Namen für Organisationseinheiten und Konten ... 576
AWS-Control-Tower-Landezone, Version 2.7 ... 577
Drei neue AWS Regionen verfügbar ... 579
Regiert nur ausgewählte Regionen ... 579
AWS Control Tower erweitert jetzt die Governance auf bestehende Organisationseinheiten in Ihren AWS Organisationen ... 580
AWS Control Tower bietet Bulk-Kontoaktualisierungen ... 580
Januar — Dezember 2020 ... 581
Die AWS Control Tower Tower-Konsole ist jetzt mit externen AWS Konfigurationsregeln verknüpft ... 581
AWS Control Tower jetzt in weiteren Regionen verfügbar ... 582
Aktualisierung von Guardrail ... 583
Die AWS Control Tower Tower-Konsole zeigt mehr Details zu OUs und Konten ... 583
Verwenden Sie AWS Control Tower, um neue AWS Umgebungen mit mehreren Konten einzurichten in AWS Organizations ... 583

Anpassungen für die AWS Control Tower Tower-Lösung 584
Allgemeine Verfügbarkeit von AWS Control Tower Version 2.3 585
Kontobereitstellung in einem Schritt in AWS Control Tower 586
Tool zur Außerbetriebnahme von AWS Control Tower 586
Benachrichtigungen zu Ereignissen im Lebenszyklus von AWS Control Tower 587
Januar — Dezember 2019 587
Allgemeine Verfügbarkeit von AWS Control Tower Version 2.2 588
Neue Wahlkontrollen in AWS Control Tower 588
Neue Detektivkontrollen in AWS Control Tower 589
AWS Control Tower akzeptiert E-Mail-Adressen für gemeinsam genutzte Konten mit anderen Domänen als dem Verwaltungskonto 590
Allgemeine Verfügbarkeit von AWS Control Tower Version 2.1 590
Dokumentverlauf 592
AWS Glossar 612
..... dcxiii

Was ist AWS Control Tower?

AWS Control Tower bietet eine einfache Möglichkeit, eine Umgebung mit AWS mehreren Konten einzurichten und zu verwalten, indem es die vorgeschriebene bewährte Methode befolgt. AWS Control Tower orchestriert die Funktionen mehrerer anderer AWS -Services, einschließlich AWS Organizations AWS Service Catalog, und AWS IAM Identity Center, um eine Landing Zone in weniger als einer Stunde aufzubauen. Ressourcen werden in Ihrem Namen eingerichtet und verwaltet.

Die AWS Control Tower-Orchestrierung erweitert die Funktionen von AWS Organizations. Um Ihre Organisationen und Konten vor Abweichungen zu schützen, was von bewährten Methoden abweicht, wendet AWS Control Tower Kontrollen an (manchmal auch als Integritätsschutz bezeichnet). Sie können beispielsweise Steuerelemente verwenden, um sicherzustellen, 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 Bereitstellung von Konten und die Kontoverwaltung erleichtert. Sie können AWS Control Tower als Ihre primäre Methode zur Bereitstellung von Konten und Infrastruktur einsetzen. Mit AWS Control Tower können Sie Unternehmensstandards einfacher einhalten, gesetzliche Anforderungen erfüllen und bewährte Methoden befolgen.

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

Kurz gesagt bietet AWS Control Tower die einfachste Möglichkeit, eine sichere, konforme AWS Umgebung mit mehreren Konten einzurichten und zu verwalten, die auf bewährten Methoden basiert, die sich aus der Zusammenarbeit mit Tausenden von Unternehmen ergeben. 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: Anleitung zu bewährten Methoden.

Features

AWS Control Tower verfügt über die folgenden Funktionen:

- Landing Zone – Eine Landing Zone ist eine gut strukturierte Umgebung mit mehreren Konten, die auf bewährten Methoden für Sicherheit und Compliance basiert. Es ist der unternehmensweite Container, der alle Ihre Organisationseinheiten (OUs), Konten, Benutzer und andere Ressourcen enthält, die Sie der Compliance-Vorschriften unterliegen möchten. Landing Zones sind skalierbar, sodass sie den Anforderungen von Unternehmen aller Größen gerecht werden können.
- Kontrollen – Eine Kontrolle (manchmal auch als Integritätsschutz bezeichnet) ist eine Regel auf hoher Ebene, die eine kontinuierliche Steuerung für Ihre gesamte AWS Umgebung bietet. Sie sind in Klartext. Es gibt drei Arten von Kontrollen: präventiv, detektivisch und proaktiv. Für Kontrollen gelten drei Kategorien von Leitlinien: obligatorisch, dringend empfohlen oder elektive . Weitere Informationen zu Kontrollen finden Sie unter Wie funktionieren Steuerungen.
- Account Factory – Eine Account Factory ist eine konfigurierbare Kontovorlage, mit der die Bereitstellung neuer Konten mit vorab genehmigten Kontokonfigurationen standardisiert werden kann. AWS Control Tower bietet eine integrierte Account Factory, mit der der Workflow zur Kontobereitstellung in Ihrer Organisation automatisiert werden kann. Weitere Informationen finden Sie unter Konten mit Account Factory bereitstellen und verwalten.
- Dashboard – Das Dashboard bietet Ihrem Team zentraler Cloud-Administratoren eine kontinuierliche Überwachung Ihrer Landing Zone. Verwenden Sie das Dashboard, um bereitgestellte Konten in Ihrem Unternehmen, Kontrollen, die für die Durchsetzung von Richtlinien aktiviert sind, Kontrollen, die für die kontinuierliche Erkennung von Richtlinienkonformität aktiviert sind, und nicht konforme Ressourcen anzuzeigen, die nach Konten und OUs organisiert sind.

Wie AWS Control Tower mit anderen - AWS Services interagiert

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

Sie können AWS Control Tower in andere - AWS Services in eine Lösung integrieren, die Sie bei der Migration Ihrer vorhandenen Workloads zu unterstützt AWS. Weitere Informationen finden Sie unter So nutzen Sie AWS Control Tower und CloudEndure für die Migration von Workloads zu AWS.

Konfiguration, Governance und Erweiterbarkeit

- Automatisierte Kontokonfiguration: AWS Control Tower automatisiert die Bereitstellung und Registrierung von Konten mithilfe einer Account Factory (oder „Verkäufermaschine“, die als Abstraktion auf der Grundlage der bereitgestellten Produkte in erstellt wurde AWS Service Catalog.

Die Account Factory kann AWS Konten erstellen und registrieren und automatisiert die Anwendung von Kontrollen und Richtlinien auf diese Konten.

- Zentralisierte Verwaltung: Durch die Nutzung der Funktionen von richtet AWS OrganizationsAWS Control Tower ein Framework ein, das eine konsistente Compliance und Governance in Ihrer Umgebung mit mehreren Konten gewährleistet. Der AWS Organizations Service bietet wesentliche Funktionen für die Verwaltung einer Umgebung mit mehreren Konten, darunter zentrale Verwaltung und Verwaltung von Konten, Kontoerstellung über AWS Organizations APIs und Service-Kontrollrichtlinien (SCPs).

- Erweiterbarkeit: Sie können Ihre eigene AWS Control Tower-Umgebung erstellen oder erweitern AWS Organizations, indem Sie direkt in , sowie in der AWS Control Tower-Konsole arbeiten. Sie können Ihre Änderungen in AWS Control Tower sehen, nachdem Sie Ihre vorhandenen Organisationen registriert und Ihre vorhandenen Konten bei AWS Control Tower registriert haben. Sie können Ihre Landing Zone von AWS Control Tower so aktualisieren, dass sie Ihren Änderungen entspricht. Wenn Ihre Workloads erweiterte Funktionen erfordern, können Sie zusammen mit AWS Control Tower andere AWS Partnerlösungen nutzen.

Verwenden Sie AWS Control Tower zum ersten Mal?

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

1. Weitere Informationen zum Planen und Organisieren Ihrer Landing Zone finden Sie unter Planen Ihrer Landing Zone von AWS Control Tower und AWS Strategie für mehrere Konten für Ihre Landing Zone von AWS Control Tower.
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 zum Aktualisieren Ihrer Landing Zone und Mitgliedskonten finden Sie unter Verwaltung 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.
- Sicherheits-OU — Diese Organisationseinheit enthält die Konten Log Archive und Audit. Diese Konten werden häufig als gemeinsam genutzte Konten bezeichnet. Wenn Sie Ihre landing zone starten, können Sie benutzerdefinierte Namen für diese gemeinsamen Konten wählen, und Sie haben die Möglichkeit, bestehende AWS Konten aus Sicherheits- und Protokollierungsgründen in AWS Control Tower zu integrieren. Diese können jedoch später nicht umbenannt werden, und bestehende Konten können aus Sicherheits- und Protokollierungsgründen nach dem ersten Start nicht hinzugefügt werden.
- 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 AWS-Workloads ausführen.
- IAM Identity Center-Verzeichnis — In diesem Verzeichnis sind Ihre IAM Identity Center-Benutzer gespeichert. Es definiert den Umfang der Berechtigungen für jeden IAM Identity Center-Benutzer.
- 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:

- Erstellt zwei AWS Organizations Organisationseinheiten (OUs): Sicherheit und Sandbox (optional), die innerhalb der organisatorischen Stammstruktur enthalten sind.
- Erstellt zwei gemeinsame Konten in der Sicherheits-OU oder fügt sie hinzu: das Log Archive-Konto und das Audit-Konto.

- 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 Protokollarchivkonto.

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 Prüfungskonto.

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 angemeldet. CloudTrail 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 AWS CloudFormation Vorlagen Ressourcen, die in Ihren Konten eingesetzt würden.

Für diejenigen, die es wissen AWS: In AWS Control Tower werden präventive Kontrollen mit Service Control Policies (SCPs) implementiert. Detektivkontrollen werden mit AWS Config Regeln implementiert. Proaktive Kontrollen werden mit AWS CloudFormation Hooks implementiert.

Verwandte Themen

- Abweichungen im AWS Control Tower erkennen und beheben

So funktioniert AWS Control Tower mit StackSets

AWS Control Tower verwendet AWS CloudFormation StackSets , um Ressourcen in Ihren Konten einzurichten. 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 AWS 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 AWS 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, AWS 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 AWS 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 AWS CloudFormation Benutzerhandbuch.

Terminologie

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

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

- Weitere Informationen zu Organisationen und Organisationseinheiten finden Sie unter AWS Organizations Terminologie und Konzepte. Wenn Sie mit AWS Control Tower noch nicht vertraut sind, ist diese Terminologie ein guter Anfang.
- AWS Organizationsist ein AWS Service, der Ihnen hilft, Ihre Umgebung zentral zu verwalten, während Sie wachsen und Ihre Workloads skalieren. AWS AWS Control Tower stützt sich AWS Organizations auf die Erstellung von Konten, die Durchsetzung präventiver Kontrollen auf OU-Ebene und die zentrale Abrechnung.
- Ein AWS Account Factory-Konto ist ein AWS Konto, das mit Account Factory in AWS Control Tower bereitgestellt wird. Manchmal wird Account Factory informell als „Verkaufsautomat“ für Konten bezeichnet.
- Ihre AWS Control Tower Tower-Heimatregion ist die AWS Region, in der Ihre AWS Control Tower Tower-Landezone bereitgestellt wurde. Du kannst deine Heimatregion in deinen landing zone Zone-Einstellungen einsehen.
- AWS Service Catalogermöglicht es Ihnen, häufig bereitgestellte IT-Services zentral zu verwalten. Im Rahmen dieses Dokuments verwendet AWS Service Catalog Account Factory die Bereitstellung neuer AWS Konten, einschließlich Konten aus benutzerdefinierten Blueprints.
- AWS CloudFormation StackSetssind eine Art von Ressource, die 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-Instanz ist ein Verweis 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 in einem einzigen Konto 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 organisationsübergreifend in einem

Unternehmen eingesetzt werden können. AWS Organizations Sie können ein Conformance Pack verwenden, um Ihre AWS Control Tower Tower-Umgebung anzupassen. Technische Blogs mit weiteren Einzelheiten finden Sie unter Verwandte Informationen.

- 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. Die aufgerufene Baseline `AWSControlTowerBaseline` ist beispielsweise verfügbar, um Ihnen bei der Registrierung Ihrer Organisationseinheiten bei AWS Control Tower zu helfen. Bei der Einrichtung und Aktualisierung der landing zone kann das Basisziel ein gemeinsames Konto oder eine spezifische Einstellung für die gesamte landing zone sein.
- Blueprint: Ein Blueprint ist ein Artefakt, das einige Metadaten kapselt, die Infrastrukturkomponenten beschreiben, die innerhalb eines Kontos bereitgestellt werden. Eine AWS CloudFormation Vorlage kann beispielsweise als Blaupause für ein AWS Control Tower Tower-Konto dienen.
- Drift: Eine Änderung an einer Ressource, die von AWS Control Tower installiert und konfiguriert wurde. Ressourcen ohne Drift sorgen dafür, dass AWS Control Tower ordnungsgemäß funktioniert.
- Nicht konforme 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 Protokollarchiv-Konto und das Audit-Konto. Sie können bei der Einrichtung benutzerdefinierte Namen für das Protokollarchiv-Konto und das Audit-Konto wählen.
- Mitgliedskonto: Ein Mitgliedskonto gehört der AWS Control Tower Tower-Organisation. Das Mitgliedskonto kann bei AWS Control Tower registriert oder abgemeldet werden. Wenn eine registrierte Organisationseinheit eine Mischung aus registrierten und nicht registrierten Konten enthält:
  - Präventive Kontrollen, die in der Organisationseinheit aktiviert sind, gelten für alle Konten innerhalb der Organisationseinheit, auch für Konten, die nicht registriert sind. Dies ist richtig, da präventive Kontrollen bei SCPs auf OU-Ebene und nicht auf Kontoebene durchgesetzt werden. Weitere Informationen finden Sie in der Dokumentation unter Vererbung von Richtlinien zur Dienstkontrolle. AWS Organizations
  - Detective Controls, die auf der Organisationseinheit aktiviert sind, gelten nicht für Konten, für die die Registrierung aufgehoben wurde.

Ein Konto kann jeweils nur Mitglied einer Organisation sein, und die 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 über den Account Factory Factory-Bereitstellungsprozess erstellt wurden, sind AWS Konten. AWS Konten können auch über die Kontoregistrierung oder die Registrierung der Organisationseinheit zu AWS Control Tower hinzugefügt werden.
- Kontrolle: Eine Kontrolle (auch als Leitplanke bezeichnet) ist eine Regel auf hoher Ebene, die eine kontinuierliche Steuerung Ihrer gesamten AWS Control Tower Tower-Umgebung gewährleistet. Jede Kontrolle erzwingt eine einzelne Regel. Präventive Kontrollen werden mit SCPs implementiert. Detektivkontrollen werden mit AWS Config Regeln implementiert. Proaktive Kontrollen werden mit AWS CloudFormation Hooks implementiert. Weitere Informationen finden Sie unter Wie funktionieren Steuerungen.
- landing zone: 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.
- Verschachtelte OU: Eine verschachtelte OU in AWS Control Tower ist eine OU, die in einer anderen OU 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 einer der Organisationseinheiten in der Hierarchie eine Richtlinie zuordnen, fließt sie nach unten und wirkt sich auf alle untergeordneten Organisationseinheiten und Konten aus. Eine verschachtelte OU-Hierarchie in AWS Control Tower kann maximal fünf Ebenen tief sein.
- Übergeordnete Organisationseinheit: Die Organisationseinheit, die in der Hierarchie unmittelbar über der aktuellen Organisationseinheit steht. 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: In AWS Control Tower kann die Hierarchie der verschachtelten Organisationseinheiten bis zu fünf Ebenen haben. Die Reihenfolge der Verschachtelung wird als Ebenen bezeichnet. Die oberste Ebene der Hierarchie wird als Ebene 1 bezeichnet.
- Organisationseinheit der obersten Ebene: Eine Organisationseinheit der obersten Ebene ist jede Organisationseinheit, die sich direkt unter dem Stamm befindet, nicht unter dem Stamm selbst. Die Stammorganisation wird nicht als Organisationseinheit betrachtet.

Preisgestaltung

Für die Nutzung von AWS Control Tower fallen keine zusätzlichen Gebühren an. Sie zahlen nur für die von AWS Control Tower aktivierten AWS Services und die Services, die Sie in Ihrer Landing Zone verwenden. Sie zahlen beispielsweise für Service Catalog für die Bereitstellung von Konten mit Account Factory und AWS CloudTrail für Ereignisse, die in Ihrer Landing Zone verfolgt werden. Informationen zu den Preisen und Gebühren für AWS Control Tower finden Sie unter AWS Control Tower – Preise.

Wenn Sie kurzlebige Workloads von Konten in AWS Control Tower ausführen, können die Kosten für steigen AWS Config. Weitere Details finden Sie unter AWS Config -Preise. Wenden Sie sich an Ihren - AWS Kundenbetreuer, um spezifischere Informationen zur Verwaltung dieser Kosten zu erhalten. Weitere Informationen zur AWS Config Funktionsweise von mit AWS Control Tower finden Sie unter Überwachen von 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 entscheiden, die von AWS Control Tower verwaltet werden. Wir empfehlen nicht, externe Trails einzurichten, es sei denn, Sie haben eine bestimmte Anforderung. Wenn Sie sich bei der Einrichtung oder Aktualisierung der Landing Zone anmelden möchten, richtet AWS Control Tower einen CloudTrail Trail auf Organisationsebene für Sie im Verwaltungskonto ein und aktiviert ihn. Weitere Informationen zur CloudTrail Kostenverwaltung finden Sie unter Verwalten von CloudTrail Kosten.

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

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.

Melde dich an für eine AWS-Konto

Wenn Sie noch keine haben AWS-Konto, führen Sie die folgenden Schritte aus, um eine zu erstellen.

Um sich für eine anzumelden AWS-Konto

1. Öffnen Sie https://portal.aws.amazon.com/billing/signup.
2. Folgen Sie den Online-Anweisungen.

   Bei der Anmeldung müssen Sie auch einen Telefonanruf entgegennehmen und einen Verifizierungscode über die Telefontasten eingeben.

   Wenn Sie sich für eine anmelden AWS-Konto, Root-Benutzer des AWS-Kontoswird eine erstellt. Der Root-Benutzer hat Zugriff auf alle AWS-Services und Ressourcen des Kontos. Aus Sicherheitsgründen sollten Sie einem Benutzer Administratorzugriff zuweisen und nur den Root-Benutzer verwenden, um Aufgaben auszuführen, für die Root-Benutzerzugriff erforderlich ist.

AWS sendet Ihnen nach Abschluss des Anmeldevorgangs eine Bestätigungs-E-Mail. Sie können jederzeit Ihre aktuelle Kontoaktivität anzeigen und Ihr Konto verwalten. Rufen Sie dazu https://aws.amazon.com/ auf und klicken Sie auf Mein Konto.

Erstellen Sie einen Benutzer mit Administratorzugriff

Nachdem Sie sich für einen angemeldet haben AWS-Konto, sichern Sie Ihren Root-Benutzer des AWS-Kontos AWS IAM Identity Center, aktivieren und erstellen Sie einen Administratorbenutzer, sodass Sie den Root-Benutzer nicht für alltägliche Aufgaben verwenden.

Sichern Sie Ihre Root-Benutzer des AWS-Kontos

1. Melden Sie sich AWS Management Consoleals Kontoinhaber an, indem Sie Root-Benutzer auswählen und Ihre AWS-Konto E-Mail-Adresse eingeben. Geben Sie auf der nächsten Seite Ihr Passwort ein.

   Hilfe bei der Anmeldung mit dem Root-Benutzer finden Sie unter Anmelden als Root-Benutzer im AWS-Anmeldung Benutzerhandbuch zu.
2. Aktivieren Sie die Multi-Faktor-Authentifizierung (MFA) für den Root-Benutzer.

   Anweisungen finden Sie unter Aktivieren eines virtuellen MFA-Geräts für Ihren AWS-Konto Root-Benutzer (Konsole) im IAM-Benutzerhandbuch.

Erstellen Sie einen Benutzer mit Administratorzugriff

1. Aktivieren Sie das IAM Identity Center.

   Anweisungen finden Sie unter Aktivieren AWS IAM Identity Center im AWS IAM Identity Center Benutzerhandbuch.
2. Gewähren Sie einem Benutzer in IAM Identity Center Administratorzugriff.

   Ein Tutorial zur Verwendung von IAM-Identity-Center-Verzeichnis als Identitätsquelle finden Sie unter Benutzerzugriff mit der Standardeinstellung konfigurieren IAM-Identity-Center-Verzeichnis im AWS IAM Identity Center Benutzerhandbuch.

Melden Sie sich als Benutzer mit Administratorzugriff an

- Um sich mit Ihrem IAM-Identity-Center-Benutzer anzumelden, verwenden Sie die Anmelde-URL, die an Ihre E-Mail-Adresse gesendet wurde, als Sie den IAM-Identity-Center-Benutzer erstellt haben.

  Hilfe bei der Anmeldung mit einem IAM Identity Center-Benutzer finden Sie im AWS-Anmeldung Benutzerhandbuch unter Anmeldung beim AWS Zugriffsportal.

Weisen Sie weiteren Benutzern Zugriff zu

1. Erstellen Sie in IAM Identity Center einen Berechtigungssatz, der der bewährten Methode zur Anwendung von Berechtigungen mit den geringsten Rechten folgt.

   Anweisungen finden Sie im Benutzerhandbuch unter Einen Berechtigungssatz erstellen.AWS IAM Identity Center
2. Weisen Sie Benutzer einer Gruppe zu und weisen Sie der Gruppe dann Single Sign-On-Zugriff zu.

   Anweisungen finden Sie im AWS IAM Identity Center Benutzerhandbuch unter Gruppen hinzufügen.

> **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. Gehen Sie wie folgt vor, wenn Sie bereit sind, Ihre Landing Zone mithilfe der AWS Control TowerAPIsKonsole oder APIs einzurichten.

Wenn Sie derzeit - AWS Kunde, aber noch nicht mit AWS Control Tower vertraut sind, sollten Sie den Abschnitt mit dem Namen lesenPlanen Ihrer Landing Zone von AWS Control Tower, bevor Sie fortfahren.

Themen

- Schnellstartanleitung für AWS Control Tower
- Voraussetzung: Automatisierte Vorab-Startprüfungen für Ihr Verwaltungskonto
- Erste Schritte mit AWS Control Tower von der Konsole aus
- Erste Schritte mit AWS Control Tower mithilfe von APIs
- Nächste Schritte

Schnellstartanleitung für AWS Control Tower

Wenn Sie noch nicht mit vertraut sind AWS, können Sie die Schritte in diesem Abschnitt ausführen, um schnell mit AWS Control Tower zu beginnen. Wenn Sie Ihre AWS Control Tower-Umgebung lieber sofort anpassen möchten, finden Sie weitere Informationen unter Schritt 2. Konfiguriere und starte deine landing zone .

> **Note**
>
> AWS Control Tower richtet kostenpflichtige Services wie AWS CloudTrail, AWS Config, Amazon , CloudWatch Amazon S3 und Amazon VPC ein. Bei Verwendung können für diese Services Kosten anfallen, wie auf der Preisseite angezeigt. Die - AWS Managementkonsole zeigt Ihnen die Nutzung aller kostenpflichtigen Services und die entstehenden Kosten an. AWS Control Tower selbst verursacht keine zusätzlichen Kosten.

Bevor Sie beginnen

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

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

Beim Schnellstartverfahren wird davon ausgegangen, dass Sie die Standardwerte für die Ressourcen in Ihrer AWS Control Tower-Umgebung akzeptieren. Viele dieser Optionen können später geändert werden. Einige einmalige Auswahlmöglichkeiten sind im Abschnitt mit dem Namen aufgeführt Erwartungen an die Konfiguration der landing zone .

Wenn Sie ein neues AWS Konto erstellt haben, erfüllt es automatisch die erforderlichen Voraussetzungen für die Einrichtung von AWS Control Tower. Sie können die folgenden Schritte ausführen.

Schnellstartschritte

1. Melden Sie sich bei der - AWS Managementkonsole mit Ihren Administratorbenutzer-Anmeldeinformationen an.
2. Navigieren Sie zur AWS Control Tower-Konsole unter https://console.aws.amazon.com/controltower.
3. Stellen Sie sicher, dass Sie in Ihrer gewünschten Heimatregion arbeiten.
4. Wählen Sie Landing Zone einrichten aus.
5. Folgen Sie den Anweisungen in der Konsole und akzeptieren Sie alle Standardwerte. Sie müssen die E-Mail-Adresse für Ihr Konto, ein Protokollarchivkonto und ein Auditkonto eingeben.
6. Bestätigen Sie Ihre Auswahl und wählen Sie Landing Zone einrichten aus.
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, Ihre Umgebung anzupassen, finden Sie in den nächsten Themen.

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

Voraussetzung: Automatisierte Vorab-Startprüfungen für Ihr Verwaltungskonto

Bevor AWS Control Tower die Landing Zone einrichtet, führt es automatisch eine Reihe von Vorabprüfungen in Ihrem Konto durch. Für diese Prüfungen sind von Ihrer Seite keine Maßnahmen erforderlich, die sicherstellen, dass Ihr Verwaltungskonto für die Änderungen bereit ist, die Ihre Landing Zone einrichten. Hier sind die Prüfungen, die AWS Control Tower vor der Einrichtung einer Landing Zone ausführt:

- Die vorhandenen Service-Limits für das AWS-Konto müssen ausreichend sein, damit AWS Control Tower gestartet werden kann. Weitere Informationen finden Sie unter Einschränkungen und Kontingente in AWS Control Tower.
- Der AWS-Konto muss die folgenden AWS Services 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 (IAM)
  - 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 Region des IAM Identity Center übereinstimmen.
- IAM Identity Center kann nur im Verwaltungskonto einer Organisation installiert werden.
- Für Ihr IAM-Identity-Center-Verzeichnis gelten drei Optionen, basierend auf der von Ihnen ausgewählten Identitätsquelle:
  - 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 stellt den Zugriff auf diese Gruppen für den von Ihnen ausgewählten Benutzer für Mitgliedskonten bereit.
  - 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 keine Benutzer oder Gruppen neuen AWS Konten zu.
  - Externer Identitätsanbieter: Wenn IAM Identity Center für AWS Control Tower mit einem externen Identitätsanbieter (IdP) eingerichtet ist, erstellt AWS Control Tower Gruppen im IAM Identity Center-Verzeichnis und stellt den Zugriff auf diese Gruppen für den Benutzer bereit, den Sie für Mitgliedskonten auswählen. Sie können bei der Kontoerstellung einen vorhandenen Benutzer aus Ihrem externen IdP in Account Factory angeben, und AWS Control Tower gibt diesem Benutzer Zugriff auf das neu verkaufte Konto, wenn es Benutzer mit demselben Namen zwischen IAM Identity Center und dem externen IdP synchronisiert. Sie können auch Gruppen in Ihrem externen IdP erstellen, die den Namen der Standardgruppen in AWS Control Tower entsprechen. Wenn Sie diesen Gruppen Benutzer zuweisen, haben diese Benutzer Zugriff auf Ihre registrierten Konten.

Weitere Informationen zum Arbeiten 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 das AWS-Konto kann der vertrauenswürdige Zugriff im Organisationsverwaltungskonto für AWS Config oder nicht aktiviert sein CloudTrail. Informationen zum Deaktivieren des vertrauenswürdigen Zugriffs finden Sie in der AWS Organizations Dokumentation zum Aktivieren oder Deaktivieren des vertrauenswürdigen Zugriffs.
- Wenn Sie bereits über einen AWS Config Recorder, einen Übermittlungskanal oder eine Aggregationseinrichtung in vorhandenen Konten verfügen, die Sie bei AWS Control Tower registrieren möchten, 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-Verwaltungskonto beim Start der Landing Zone. Weitere Informationen finden Sie unter Registrieren von Konten mit vorhandenen AWS Config Ressourcen.
- Wenn Sie kurzlebige Workloads von Konten in AWS Control Tower ausführen, können die mit AWS Config verbundenen Kosten steigen. Wenden Sie sich an Ihren - AWS Kundenbetreuer, um spezifischere Informationen zur Verwaltung dieser Kosten zu erhalten.
- Wenn Sie ein Konto bei AWS Control Tower registrieren, wird Ihr Konto durch den AWS CloudTrail Trail für die AWS Control Tower-Organisation geregelt. Wenn Sie bereits eine Bereitstellung eines CloudTrail Trails im Konto haben, werden möglicherweise doppelte Gebühren angezeigt, es sei denn, Sie löschen den vorhandenen Trail für das Konto, bevor Sie ihn in 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 Regionen aktiviert werden, die von AWS Control Tower verwaltet werden. Andernfalls kann der Start während des Konfigurationsprozesses fehlschlagen.

Erste Schritte mit AWS Control Tower von der Konsole aus

Dieses Verfahren für die ersten Schritte richtet sich an AWS Control Tower Tower-Administratoren. Gehen Sie wie folgt vor, wenn Sie bereit sind, Ihre landing zone mithilfe der AWS Control Tower Tower-Konsole einzurichten. Von Anfang bis Ende sollte es etwa eine halbe Stunde dauern. Dieses Verfahren erfordert einige Voraussetzungen und drei Hauptschritte.

Wenn Sie derzeit AWS Kunde sind, aber noch nicht bei AWS Control Tower sind, sollten Sie den genannten Abschnitt lesenPlanen Ihrer Landing Zone von AWS Control Tower, bevor Sie fortfahren.

Themen

- Schritt 1: Erstellen Sie die E-Mail-Adressen für Ihr gemeinsames Konto
- Erwartungen an die Konfiguration der landing zone
- Schritt 2. Konfiguriere und starte deine landing zone
- Schritt 3. Überprüfen und richten Sie die landing zone ein

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

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

- Um Ihre landing zone 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 kollaborativer Posteingang — ein gemeinsames E-Mail-Konto —, das für die verschiedenen Benutzer in Ihrem Unternehmen bestimmt ist, die spezifische Aufgaben im Zusammenhang mit AWS Control Tower ausführen.
- Wenn Sie AWS Control Tower zum ersten Mal einrichten und bestehende Sicherheits- und Protokollarchivkonten in AWS Control Tower importieren, 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 Team von Benutzern vorgesehen, die Zugriff auf die von AWS Control Tower zur Verfügung gestellten Prüfungsinformationen benötigen. Sie können dieses Konto auch als Zugriffspunkt für Tools von Drittanbietern verwenden, die eine programmatische Prüfung der Umgebung auf Konformität durchführt
- Protokollarchivkonto — Dieses Konto ist für Ihr Team von Benutzern bestimmt, die Zugriff auf alle Protokollinformationen für alle Ihre registrierten Konten innerhalb registrierter Organisationseinheiten 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 bei der Durchführung von Aktionen in diesen Konten einen IAM Identity Center-Benutzer mit den entsprechenden Zugriffsberechtigungen verwenden.

> **Note**
>
> Wenn Sie bestehende AWS Konten als Ihre Audit - und Protokollarchiv-Konten angeben, müssen die vorhandenen Konten vor dem Start einige Prüfungen bestehen, um sicherzustellen, dass keine Ressourcen im Konflikt mit den AWS Control Tower Tower-Anforderungen stehen. Wenn diese Prüfungen nicht erfolgreich sind, ist Ihre Landezoneneinrichtung möglicherweise nicht erfolgreich. Insbesondere dürfen die Konten nicht über vorhandene AWS Config Ressourcen verfügen. Weitere Informationen finden Sie unter Überlegungen zur Mitnahme vorhandener Sicherheits- oder Protokollkonten.

Aus Gründen der Übersichtlichkeit werden in diesem Benutzerhandbuch die gemeinsam genutzten Konten immer mit ihren Standardnamen bezeichnet: Log Archive und Audit. Denken Sie beim Lesen dieses Dokuments daran, die benutzerdefinierten Namen, die Sie diesen Konten zunächst geben, zu ersetzen, wenn 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 Tower-Organisationseinheiten (OUs), um sie an die AWS Multi-Account-Strategie anzupassen. Möglicherweise stellen Sie während der Umstellung einige Inkonsistenzen fest, um die Klarheit dieser Namen zu verbessern. Die Security OU wurde früher als Core OU bezeichnet. Die Sandbox-Organisationseinheit wurde früher als benutzerdefinierte Organisationseinheit bezeichnet.

Erwartungen an die Konfiguration der 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 nach der Einrichtung nicht geändert werden.

Wichtige Elemente, die während der Einrichtung konfiguriert werden müssen

- Sie können Ihre OU-Namen der obersten Ebene während der Einrichtung auswählen und Sie können auch die OU-Namen ändern, nachdem Sie Ihre landing zone 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 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 können Sie optional vorhandene AWS Konten für AWS Control Tower angeben, die als Audit- und Protokollarchivkonten verwendet werden sollen. Wenn Sie beabsichtigen, bestehende AWS Konten anzugeben, 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. (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.
- Sie können optional einen zuvor definierten Blueprint angeben, der für die Bereitstellung benutzerdefinierter Mitgliedskonten von der AWS Control Tower Tower-Konsole aus verwendet werden soll. Sie können Konten später anpassen, wenn Ihnen kein Blueprint zur Verfügung steht. Siehe Passen Sie Konten mit Account Factory Customization (AFC) an.

Konfigurationsoptionen, die nicht rückgängig gemacht werden können

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

Schritt 2. Konfiguriere und starte deine landing zone

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

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

Erfahre, wie du deine landing zone mit dem AWS CLI In konfigurierst und startestErste Schritte mit AWS Control Tower mithilfe von APIs.

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

Vorbereiten: Navigieren Sie zur AWS Control Tower Tower-Konsole

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

Schritt 2a. Überprüfe deine AWS Regionen und wähle sie aus

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

In diesem Abschnitt des Einrichtungsprozesses können Sie weitere 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 AWS Regionen für die Verwaltung auszuwählen

1. Das Fenster zeigt Ihnen die aktuelle Regionsauswahl. Öffnen Sie das Drop-down-Menü, um eine Liste zusätzlicher Regionen zu sehen, die für die Verwaltung verfügbar sind.

2. Markieren Sie das Kästchen neben jeder Region, um die Verwaltung durch AWS Control Tower zu übernehmen. 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 für die Steuerung „Region Deny Control“ die Option Aktiviert aus. Standardmäßig ist die Einstellung für dieses Steuerelement Nicht aktiviert.

Schritt 2b. Konfigurieren Sie Ihre Organisationseinheiten (OUs)

Wenn Sie die Standardnamen dieser Organisationseinheiten akzeptieren, müssen Sie nichts weiter unternehmen, um mit der Einrichtung fortzufahren. Um die Namen der Organisationseinheiten zu ändern, geben Sie die neuen Namen direkt in das Formularfeld ein.

- Foundational OU — AWS Control Tower basiert auf einer Foundational OU, die ursprünglich Security OU genannt wurde. Sie können den Namen dieser OU bei der Ersteinrichtung und danach auf der Seite mit den OU-Details ändern. Diese Sicherheits-OU 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 Ihnen, neben der Sicherheits-OU mindestens eine zusätzliche Organisationseinheit in Ihrer landing zone bereitzustellen. Wenn diese zusätzliche Organisationseinheit für Entwicklungsprojekte vorgesehen ist, empfehlen wir, sie als Sandbox-Organisationseinheit zu bezeichnen, wie in der Richtlinien für die Einrichtung einer gut strukturierten Umgebung angegeben. Wenn Sie bereits über eine bestehende Organisationseinheit in AWS Organizations verfügen, wird Ihnen möglicherweise die Option angezeigt, die Einrichtung einer zusätzlichen Organisationseinheit in AWS Control Tower zu überspringen.

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

In diesem Abschnitt des Einrichtungsprozesses zeigt das Panel die Standardauswahl für die Namen Ihrer gemeinsam genutzten AWS Control Tower Tower-Konten. Diese Konten sind ein wesentlicher Bestandteil Ihrer landing zone. Verschieben oder löschen Sie diese gemeinsamen Konten nicht. Sie können bei der Einrichtung benutzerdefinierte Namen für die Konten für die Audit - und Protokollarchive wählen. Alternativ haben Sie die einmalige Möglichkeit, bestehende AWS Konten als Ihre gemeinsamen Konten anzugeben.

Sie müssen eindeutige E-Mail-Adressen für Ihre Protokollarchiv- und 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 Tower-Verwaltungskonto ist Teil der Root-Ebene. Das Verwaltungskonto ermöglicht die Abrechnung mit AWS Control Tower. Das Konto hat auch Administratorrechte für Ihre landing zone. Sie können keine separaten Konten für die Abrechnung und für Administratorberechtigungen in AWS Control Tower 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 Konto, ob neu oder bereits vorhanden, 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.

Um die gemeinsamen Konten zu konfigurieren, geben Sie die angeforderten Informationen ein.

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 entscheiden sich dafür, es Sicherheitskonto zu nennen.
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 Protokollaufbewahrungsrichtlinie für Amazon S3 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

Standardkontenprotokollierung und 10 Jahre für die Zugriffsprotokollierung. Diese Funktion ist auch verfügbar, wenn Sie Ihre landing zone aktualisieren oder zurücksetzen.

Wahlweise können Sie den Zugriff selbst verwalten AWS-Konto

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, z. B. einem externen IdP, entweder für den direkten Kontoverbund oder für den Verbund mit mehreren Konten mithilfe von IAM Identity Center. Sie können diese Auswahl später ändern.

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.

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

Weitere Informationen finden Sie unter Anleitung zum IAM Identity Center.

Optional können Sie AWS CloudTrail Wanderwege konfigurieren

Als bewährte Methode empfehlen wir, dass Sie die Protokollierung einrichten. Wenn Sie AWS Control Tower erlauben möchten, einen CloudTrail Trail auf Organisationsebene einzurichten und diesen für Sie zu verwalten, wählen Sie Opt in. Wenn Sie die Protokollierung mit Ihren eigenen CloudTrail Trails oder einem Protokollierungstool eines Drittanbieters verwalten möchten, wählen Sie „Abmelden“. Bestätige deine Auswahl, wenn du in der Konsole dazu aufgefordert wirst. Du kannst deine Auswahl ändern und Trails auf Organisationsebene aktivieren oder deaktivieren, wenn du deine landing zone 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

Optional konfigurieren AWS KMS keys

Wenn Sie Ihre Ressourcen mit einem AWS KMS Verschlüsselungsschlüssel ver- und entschlüsseln möchten, aktivieren Sie das Kontrollkästchen. Wenn Sie bereits Schlüssel haben, können Sie diese aus den Kennungen auswählen, die in einem Drop-down-Menü angezeigt werden. Sie können einen neuen Schlüssel generieren, indem Sie Schlüssel erstellen wählen. Sie können jederzeit einen KMS-Schlüssel hinzufügen oder ändern, wenn Sie Ihre landing zone aktualisieren.

Wenn Sie landing zone 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
- Wurden der Richtlinie 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 wie im nächsten Abschnitt beschrieben zu bearbeiten.

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 einzigen JSON-Anweisung oder zeilenweise hinzufügen.

Das Verfahren beschreibt, wie die standardmäßige KMS-Schlüsselrichtlinie in der AWS KMS Konsole aktualisiert wird, indem Richtlinienanweisungen hinzugefügt werden, die die

Verschlüsselung zulassen AWS Config und CloudTrail AWS KMS für diese verwendet werden. Die Richtlinienerklärungen 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.

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 Vom Kunden verwaltete Schlüssel aus.
3. Wählen Sie in der Tabelle den Schlüssel aus, den Sie bearbeiten möchten.
4. Stellen Sie auf der Registerkarte Schlüsselrichtlinie sicher, dass Sie die Schlüsselrichtlinie einsehen können. Wenn Sie die wichtige 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:aws:kms:YOUR-HOME-REGION:YOUR-MANAGEMENT-ACCOUNT-ID:key/YOUR-KMS-KEY-ID"
}
```

   CloudTrail Grundsatzerklärung

```
{
    "Sid": "Allow CloudTrail to use KMS for encryption",
    "Effect": "Allow",
    "Principal": {
        "Service": "cloudtrail.amazonaws.com"
    },
    "Action": [
        "kms:GenerateDataKey*",
        "kms:Decrypt"
    ],
    "Resource": "arn:aws:kms:YOUR-HOME-REGION:YOUR-MANAGEMENT-ACCOUNT-ID:key/YOUR-KMS-KEY-ID",
    "Condition": {
        "StringEquals": {
            "aws:SourceArn": "arn:aws:cloudtrail:YOUR-HOME-REGION:YOUR-MANAGEMENT-ACCOUNT-ID:trail/aws-controltower-BaselineCloudTrail"
        },
        "StringLike": {
            "kms:EncryptionContext:aws:cloudtrail:arn": "arn:aws: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, mit denen CloudTrail die erforderlichen Mindestberechtigungen gewährt AWS Config werden. Die Beispielrichtlinie enthält 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:aws: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:aws:kms:YOUR-HOME-REGION:YOUR-MANAGEMENT-ACCOUNT-
ID:key/YOUR-KMS-KEY-ID",
            "Condition": {
                "StringEquals": {
                    "aws:SourceArn": "arn:aws:cloudtrail:YOUR-HOME-REGION:YOUR-
MANAGEMENT-ACCOUNT-ID:trail/aws-controltower-BaselineCloudTrail"
                },
                "StringLike": {
                    "kms:EncryptionContext:aws:cloudtrail:arn":
 "arn:aws: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 dienstverknüpften Rollen (S3 Bucket Delivery) im Entwicklerhandbuch.AWS Config

> **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 dazu zwingt, eine Aktion auszuführen, 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 mit mehreren Regionen und asymmetrische Schlüssel erstellen. AWS Control Tower unterstützt jedoch keine Schlüssel mit mehreren 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.

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

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

Optional können Sie benutzerdefinierte Mitgliedskonten konfigurieren und erstellen

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 von der AWS Control Tower Tower-Konsole aus verwendet werden soll. Sie können Konten später anpassen, wenn Ihnen kein Blueprint zur Verfügung steht. Siehe Passen Sie Konten mit Account Factory Customization (AFC) an.

Schritt 3. Überprüfen und richten Sie die landing zone ein

Der nächste Abschnitt des Setups zeigt Ihnen die Berechtigungen, die AWS Control Tower für Ihre landing zone benötigt. Wählen Sie ein Kontrollkästchen, um jedes Thema zu erweitern. Sie werden

gebeten, 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 zur Verwaltung von AWS Ressourcen und zur Durchsetzung von Regeln in meinem Namen verwenden wird.
2. Um Ihre Auswahl abzuschließen und den Start zu initialisieren, wählen Sie landing zone einrichten.

Diese Reihe von Schritten startet den Prozess der Einrichtung Ihrer landing zone, der etwa dreißig Minuten dauern kann. Während der Einrichtung erstellt AWS Control Tower Ihre Root-Ebene, die Sicherheits-OU und die gemeinsamen Konten. Andere AWS Ressourcen werden erstellt, geändert oder gelöscht.

⚠ Bestätigen Sie SNS-Abonnements

Die E-Mail-Adresse, die Sie für das Audit-Konto angegeben haben, erhält E-Mails mit AWS Benachrichtigungen und Abonnementbestätigungen aus allen AWS Regionen, die von AWS Control Tower unterstützt werden. Um Compliance-E-Mails in Ihrem Audit-Konto zu erhalten, müssen Sie in jeder E-Mail aus jeder AWS Region, die von AWS Control Tower unterstützt wird, den Link Abonnement bestätigen auswählen.

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 AWS 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 Vorab-Startprüfungen für Ihr Verwaltungskonto 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: Starte deine landing zone
- Identifizieren Sie Ihre landing zone
- Aktualisiere deine landing zone
- Setze die landing zone zurück, um Drift zu beheben
- Machen Sie Ihre landing zone außer Betrieb
- Beispiele: Einrichten einer Landing Zone von AWS Control Tower nur mit APIs
- Starten einer landing zone mit AWS 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 für AWS Control Tower angeben, die als Audit- und Protokollarchivkonten verwendet werden sollen. 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: Einrichten einer Landing Zone von AWS Control Tower nur mit APIs .

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:

- Schaffung einer neuen AWS Organizations Organisation,
- die E-Mail-Adressen für Ihr gemeinsames Konto einrichten,
- 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:

1. Rufen Sie die AWS Organizations `CreateOrganization` API auf und aktivieren Sie alle Funktionen, um die Foundational OU zu erstellen. AWS Control Tower nennt dies zunächst Security OU. Diese Sicherheits-OU enthält Ihre beiden gemeinsamen Konten, die standardmäßig als Protokollarchiv-Konto und Audit-Konto bezeichnet werden.

   ```
   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, sie als Sandbox-Organisationseinheit zu bezeichnen, wie in der AWS Strategie für mehrere Konten für Ihre Landing Zone von AWS Control Tower angegeben.

Schritt 2. Stellen Sie bei Bedarf gemeinsame Konten bereit:

Um Ihre landing zone einzurichten, benötigt AWS Control Tower zwei E-Mail-Adressen. Wenn Sie landing zone Zone-APIs verwenden, um AWS Control Tower zum ersten Mal einzurichten, müssen Sie vorhandene Sicherheits- und AWS Protokollarchivkonten verwenden. Sie können die aktuellen E-Mail-Adressen der vorhandenen verwenden AWS-Konten. Jede dieser E-Mail-Adressen dient als kollaborativer Posteingang — ein gemeinsames E-Mail-Konto — für die verschiedenen Benutzer in Ihrem Unternehmen, die spezifische Aufgaben im Zusammenhang mit AWS Control Tower ausführen.

Wenn Sie noch keine Konten haben, können Sie die Sicherheits- und AWS AWS Protokollarchivkonten mithilfe von AWS Organizations APIs bereitstellen, um mit der Einrichtung einer neuen landing zone zu beginnen.

1. Rufen Sie die AWS Organizations `CreateAccount` API auf, um das Protokollarchiv-Konto und das Audit-Konto in der Security 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"
```

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

Schritt 3. Erstellen Sie die erforderlichen Servicerollen

Erstellen Sie die folgenden IAM-Servicerollen, mit denen AWS Control Tower die API-Aufrufe ausführen kann, die für die Einrichtung Ihrer landing zone erforderlich sind:

- `AWSControlTowerAdmin`
- `AWSControlTowerCloudTrailRole`
- `AWSControlTowerStackSetRole`
- `AWSControlTowerConfigAggregatorRoleForOrganizations`

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

So erstellen Sie eine IAM-Rolle:

1. 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": [
                "controltower:CreateLandingZone",
                "controltower:UpdateLandingZone",
                "controltower:ResetLandingZone",
                "controltower:DeleteLandingZone",
```

```
                "controltower:GetLandingZoneOperation",
                "controltower:GetLandingZone",
                "controltower:ListLandingZones",
                "controltower:ListTagsForResource",
                "controltower:TagResource",
                "controltower:UntagResource",
                "servicecatalog:*",
                "organizations:*",
                "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": "*"
        }
    ]
}
```

Schritt 2: Starte deine landing zone

Die AWS Control Tower `CreateLandingZone` API erfordert eine landing zone Zone-Version und eine Manifestdatei als Eingabeparameter. Sie können die Manifestdatei verwenden, um die folgenden Funktionen zu konfigurieren:

- Konfigurieren Sie optional die Aufbewahrung von Protokollen
- Wahlweise können Sie den Zugriff selbst verwalten AWS-Konto
- Optional können Sie AWS CloudTrail Pfade konfigurieren
- Optional konfigurieren AWS KMS keys

Nachdem Sie Ihre Manifestdatei kompiliert haben, können Sie eine neue landing zone erstellen.

> **Note**
>
> AWS Control Tower unterstützt die Option „Region Deny Control“ nicht, wenn APIs zum Konfigurieren und Starten einer landing zone verwendet werden. Nachdem Sie Ihre landing zone mithilfe von APIs erfolgreich gestartet haben, können Sie mit der AWS Control Tower Tower-Konsole die Region Deny Control konfigurieren.

1. Rufen Sie die AWS Control Tower `CreateLandingZone` API auf. Diese API benötigt eine Landingzone-Version und eine Manifestdatei als Eingabe.

   ```
   aws controltower create-landing-zone --landing-zone-version 3.3 --manifest "file://
   LandingZoneManifest.json"
   ```

   Beispiel für ein LandingZoneManifestJSON-Manifest:

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

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

> **Note**
>
> Wie im Beispiel gezeigt, müssen die SecurityRoles Konten AccountIdfür CentralizedLogging und unterschiedlich sein.

Ausgabe:

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

2. Rufen Sie die `GetLandingZoneOperation` API auf, um den Status des `CreateLandingZone` Vorgangs zu überprüfen. Die `GetLandingZoneOperation` API gibt den Status `SUCCEEDEDFAILED`, oder zurück`IN_PROGRESS`.

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

Ausgabe:

```
{
    "operationDetails": {
        "operationType": "CREATE",
        "startTime": "Thu Nov 09 20:39:19 UTC 2023",
        "endTime": "Thu Nov 09 21:02:01 UTC 2023",
        "status": "SUCCEEDED"
    }
}
```

3. Wenn der Status als zurückkehrtSUCCEEDED, können Sie die GetLandingZone API aufrufen, um die Konfiguration der landing zone zu überprüfen.

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

Ausgabe:

```
{
    "landingZone": {
        "arn": "arn:aws:controltower:us-
west-2:123456789012:landingzone/1A2B3C4D5E6F7G8H",
        "driftStatus": {
            "status": "IN_SYNC"
        },
        "latestAvailableVersion": "3.3",
        "manifest": {
            "accessManagement": {
                "enabled": true
            },
            "securityRoles": {
                "accountId": "333333333333"
            },
            "governedRegions": [
                "us-west-1",
                "eu-west-3",
                "us-west-2"
            ],
            "organizationStructure": {
                "sandbox": {
                    "name": "Sandbox"
                },
                "security": {
                    "name": "CORE"
                }
            },
            "centralizedLogging": {
                "accountId": "222222222222",
                "configurations": {
                    "loggingBucket": {
                        "retentionDays": 60
                    },
```

```
                    "kmsKeyArn": "arn:aws:kms:us-west-1:123456789123:key/
e84XXXXX-6bXX-49XX-9eXX-ecfXXXXXXXXX",
                    "accessLoggingBucket": {
                        "retentionDays": 60
                    }
                },
                "enabled": true
            }
        },
        "status": "PROCESSING",
        "version": "3.3"
    }
}
```

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 landing zone Zone-Version verfügbar ist oder um andere Aktualisierungen an Ihrer landing zone Zone-Konfiguration vorzunehmen, können Sie die `UpdateLandingZone` API aufrufen und auf eine aktualisierte 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 Ihr aktualisiertes Manifest.

```
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.json:

```
{
   "governedRegions": ["us-west-2","us-west-1"],
   "organizationStructure": {
       "security": {
           "name": "CORE"
       },
       "sandbox": {
           "name": "Sandbox"
       }
   },
   "centralizedLogging": {
        "accountId": "222222222222",
        "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": "333333333333"
    },
    "accessManagement": {
        "enabled": true
    }
}
```

Ausgabe:

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

> **Optional können Sie OU erneut registrieren, um Konten zu aktualisieren**
>
> Für registrierte AWS Control Tower Tower-Organisationseinheiten mit weniger als 300 Konten können Sie über die AWS Control Tower Tower-Konsole auf die OU-Seite im Dashboard zugreifen und OU erneut registrieren 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 Sie die neueste verfügbare landing zone Zone-Version verwenden. Sie können die `GetLandingZone` API aufrufen und Ihre landing zone Zone-Version mit der neuesten verfügbaren Version vergleichen. Bei Bedarf können Sie dies tun, Aktualisiere deine landing zone damit Ihre landing zone die neueste verfügbare Version verwendet. In diesen Beispielen verwenden wir Version 3.3 als neueste Version.

1. Rufen Sie die `GetLandingZone`-API auf. Wenn die API den Drift-Status von zurückgibt`DRIFTED`, befindet sich Ihre landing zone im Driftmodus.
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.

Machen Sie Ihre landing zone 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. Exemplarische Vorgehensweise: 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"
}
```

Beispiele: Einrichten einer Landing Zone von AWS Control Tower nur mit APIs

Diese exemplarische Vorgehensweise ist ein unterstützendes Dokument. Erläuterungen, Einschränkungen und weitere Informationen finden Sie unter Erste Schritte mit AWS Control Tower unter Verwendung von APIs.

Voraussetzungen

Bevor Sie eine Landing Zone von AWS Control Tower erstellen, müssen Sie eine Organisation, zwei gemeinsam genutzte Konten und einige IAM-Rollen erstellen. Dieses Walkthrough-Tutorial enthält diese Schritte mit CLI-Befehlen und -Ausgabebeispielen.

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 >controltower_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 Landing Zone-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 dabei, die Landing Zone-Manifestdatei zu generieren.

```
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 Landing Zone mit der neuesten Version.

Sie müssen die Landing Zone 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 Landing Zone-Erstellung.

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
```

Beispielstatusausgabe:

```
{
```

```
    "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 der Operation immer wieder meldet, z. B. eine Protokolldatei. Dann müssen Sie den Befehl nicht weiter 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
```

So zeigen Sie detaillierte Informationen zu Ihrer Landing Zone an

Schritt 1. Ermitteln des ARN der Landing Zone

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

Die Ausgabe enthält die Kennung der Landing Zone, wie im folgenden Beispiel für die Ausgabe gezeigt.

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

Schritt 2. Abrufen der 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"
    }
}
```

Starten einer landing zone mit AWS CloudFormation

Sie können eine landing zone AWS CloudFormation entweder über die AWS 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 AWS CloudFormation.

Themen

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

Voraussetzungen für den Start einer landing zone mit AWS 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 unter Schritt 1: Konfiguriere deine landing zone .
2. Stellen Sie über die AWS CloudFormation Konsole oder mithilfe der AWS CLI eine AWS 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 AWS CloudFormation

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

```
Parameters:
  Version:
    Type: String
    Description: The version number of Landing Zone
  GovernedRegions:
    Type: List
    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 AWS CloudFormation

Sie können AWS CloudFormation damit eine landing zone verwalten, die Sie bereits gestartet haben, indem Sie die landing zone in einen neuen oder vorhandenen AWS 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

Nachdem Ihre Landing Zone 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 .
- Informationen zum Registrieren von Organisationen und Konten für Ihre AWS Organizations Bereitstellungen finden Sie unter Bestehende Organisationen und Konten steuern.
- Ihre Endbenutzer können ihre eigenen AWS Konten in Ihrer Landing Zone mithilfe von Account Factory bereitstellen. Weitere Informationen finden Sie unter Berechtigungen für die Konfiguration und Bereitstellung von Konten.
- Um sicherzustellenKonformitätsvalidierung für AWS Control Tower, dass Ihre zentralen Cloud-Administratoren Protokollarchive im Log-Archive-Konto überprüfen können, und bestimmte externe Prüfer können Auditinformationen im Audit-Konto (freigegeben) überprüfen, das Mitglied der Sicherheitsorganisation ist.
- Weitere Informationen zu den Funktionen von AWS Control Tower finden Sie unter Verwandte Informationen.
- Versuchen Sie, eine kuratierte Liste von YouTube Videos zu besuchen, die mehr über die Verwendung der AWS Control Tower-Funktionalität erklären.
- Von Zeit zu Zeit müssen Sie möglicherweise Ihre Landing Zone aktualisieren, um die neuesten Backend-Updates und die neuesten Kontrollen zu erhalten und Ihre Landing Zone beizubehalten up-to-date. Weitere Informationen finden Sie unter Verwaltung von Konfigurationsupdates in AWS Control Tower.
- Wenn bei der Verwendung von AWS Control Tower Probleme auftreten, finden Sie weitere Informationen unter Fehlerbehebung.

> **Important**
>
> Wenn Sie MFA noch nicht für den Stammbenutzer Ihres Kontos 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 Nutzung von AWS Control Tower beachten sollten. Wenn Sie Ihre landing zone aufgrund eines Problems mit der Servicequote nicht einrichten können, wenden Sie sich an AWS Support.

Weitere Informationen zu Einschränkungen, die für Steuerelemente spezifisch sind, finden Sie unterEinschränkungen der Kontrolle.

> **Ein neues Referenzhandbuch für Steuerungen**
>
> Informationen zu AWS Control Tower Controls wurden in das AWS Control Tower Controls Reference Guide verschoben.

Einschränkungen in AWS Control Tower

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

- AWS Control Tower hat allgemeine Einschränkungen bei der Parallelität. Im Allgemeinen ist jeweils ein Vorgang zulässig. Zwei Ausnahmen von dieser Beschränkung sind zulässig:
  - Optionale Steuerungen können über einen asynchronen Prozess gleichzeitig aktiviert und deaktiviert werden. Insgesamt können bis zu einhundert (100) steuerungsbezogene Operationen gleichzeitig ausgeführt werden, unabhängig davon, ob sie von der Konsole oder von einer API aus aufgerufen werden. Von diesen 100 Vorgängen können bis zu 20 gleichzeitig proaktive Kontrollvorgänge sein.
  - 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 Verwaltung von Konten muss jeweils für ein Konto aufgehoben werden.
- E-Mail-Adressen von gemeinsam genutzten Konten in der Security OU können geändert werden, aber Sie müssen Ihre landing zone aktualisieren, um diese Änderungen in der AWS Control Tower Tower-Konsole zu sehen.
- Für Organisationseinheiten in Ihrer AWS Control Tower Tower-Landezone gilt ein Limit von fünf (5) SCPs pro OU.

- AWS Control Tower unterstützt bis zu 10.000 Konten in der Organisation Ihrer Landing Zone, aufgeteilt auf all Ihre Organisationseinheiten.
- Bestehende Organisationseinheiten mit über 300 direkt verschachtelten Konten können nicht in AWS Control Tower registriert oder erneut registriert werden. Weitere Informationen zu Einschränkungen bei der Registrierung von Organisationseinheiten finden Sie unter. Regionen und Stapel setzen Grenzen
- Anpassungen für AWS Control Tower (cFCT) sind in diesen nicht verfügbar AWS-Regionen, da einige Abhängigkeiten nicht verfügbar sind:
  - Asien-Pazifik (Jakarta und Osaka)
  - Israel (Tel Aviv)
  - Naher Osten (VAE)
  - Europa (Spain)
  - Asien-Pazifik (Hyderabad)
  - Europa (Zürich)
  - Kanada West (Calgary)

  Sie können Ressourcen in diesen Regionen mit cFCT bereitstellen und verwalten, wenn Sie cFCT in Ihrer AWS Control Tower Tower-Heimatregion bereitstellen, aber Sie können cFCT in diesen Regionen nicht erstellen.
- AWS Control Tower Account Factory for Terraform (AFT) ist im Folgenden nicht verfügbar AWS-Regionen, da einige Abhängigkeiten nicht verfügbar sind:
  - Israel (Tel Aviv)
  - Naher Osten (VAE)
  - Europa (Spain)
  - Asien-Pazifik (Hyderabad)
  - Europa (Zürich)
  - Kanada West (Calgary)
- Die folgenden Regionen unterstützen IAM Identity Center nicht.
  - Region Naher Osten (VAE), me-central-1
  - Region Asien-Pazifik (Hyderabad), ap-south-2
  - Kanada West (Calgary), ca-west-1

Weitere Informationen zu AWS-Regionen und Support für IAM Identity Center finden Sie unter Regionen und Endpunkte im AWS Identity and Access Management-Benutzerhandbuch.

- Die folgenden Regionen unterstützen nicht. AWS Service Catalog
  - Kanada West (Calgary), ca-west-1

  Weitere Informationen zur AWS Control Tower Tower-Funktionalität in Regionen, die dies nicht unterstützen AWS Service Catalog, finden Sie unterAWS Control Tower in AWS Kanada West (Calgary) verfügbar.
- Wenn Sie eine Kontroll-API aufrufen, um eine Steuerung zu aktivieren oder zu deaktivieren, liegt das Limit für `EnableControl` und `DisableControl` Updates in AWS Control Tower bei einhundert (100) gleichzeitigen Vorgängen. Zehn Operationen (10) können gleichzeitig ausgeführt werden, wobei die verbleibenden Vorgänge in die Warteschlange gestellt werden. Möglicherweise müssen Sie Ihren Code anpassen, um auf die Fertigstellung zu warten.
- Innerhalb der Gesamtbegrenzung von 100 Kontrollvorgängen können bis zu 20 Operationen gleichzeitig proaktive Kontrollvorgänge sein.
- 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 Quotas-Konsole bietet Informationen über AWS Control Tower Tower-Kontingente. Sie können die Servicekontingenten-Konsole verwenden, um die Standard-Servicekontingenten einzusehen oder um Kontingenterhöhungen für anpassbare Kontingente anzufordern.

Die folgenden Kontingente können über die Service Quotas Quotas-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 von 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 in AWS Control Tower nicht durchgeführt werden. Weitere Informationen zur Anzahl der Konten pro Organisationseinheit

finden Sie Regionen und Stapel setzen Grenzen in der AWS Control Tower Tower-Dokumentation. Standard: 300, nicht einstellbar.

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

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

> **Note**
>
> Es kann bis zu zwei Tage dauern, bis ein Antrag auf Erhöhung des Servicekontingents wirksam wird. Stellen Sie sicher, dass Sie die Erhöhung des Kontingents von Ihrer AWS Control Tower Tower-Heimatregion aus beantragen.

Alternativ können Sie sich an den AWS Support wenden, um eine Erhöhung des Kontingents für einige Ressourcen in AWS Control Tower zu beantragen. Oder schauen Sie sich das folgende Video an und erfahren Sie, wie Sie die Erhöhung bestimmter Servicekontingenten automatisieren können.

Video: Automatisieren Sie Anfragen zur Erhöhung der Servicequote 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 in AWS Control Tower automatisiert werden kann. Es zeigt auch, wie Sie die Registrierung neuer Konten für den 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.

Video-Komplettlösung zu Quotenerhöhungen in AWS Control Tower.

Bei der Bereitstellung neuer Konten in dieser Umgebung können Sie mithilfe von Lebenszyklusereignissen automatisierte Anfragen zur Erhöhung der Servicekontingenten in bestimmten Fällen auslösen. AWS-Regionen

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

Einschränkungen der Kontrolle

> **Ein neues Referenzhandbuch für Steuerungen**
>
> Informationen zu AWS Control Tower Controls wurden in das AWS Control Tower Controls Reference Guide verschoben.

Wenn Sie AWS Control Tower-Ressourcen wie ein SCP ändern oder AWS Config Ressourcen entfernen, z. B. einen Config-Recorder oder -Aggregator, kann AWS Control Tower nicht mehr garantieren, dass die Kontrollen 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 Kontrollen auf ihre Standardkonfiguration zurückgesetzt werden, wenn Sie Ihre landing zone aktualisieren. Änderungen, die Sie möglicherweise an SCPs vorgenommen haben, werden konstruktionsbedingt durch die Standardversion der Steuerung ersetzt.

Einige Kontrollen in AWS Control Tower funktionieren in bestimmten Regionen, in AWS-Regionen denen AWS Control Tower verfügbar ist, nicht, da diese Regionen die erforderlichen zugrunde liegenden Funktionen nicht unterstützen. Diese Einschränkung betrifft bestimmte detektive Kontrollen, bestimmte proaktive Kontrollen und bestimmte Kontrollen im vom Security Hub Service verwalteten Standard: AWS Control Tower. Weitere Informationen zur regionalen Verfügbarkeit finden Sie in der Dokumentation zur Liste der regionalen Dienste und in der Referenzdokumentation zu Security Hub-Steuerelementen.

Das Kontrollverhalten ist auch bei gemischter Verwaltung begrenzt. Weitere Informationen finden Sie unter Vermeiden Sie gemischte Verwaltungsstrukturen bei der Konfiguration von Regionen.

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

Sie können die Regionen für jede Kontrolle in der AWS Control Tower Tower-Konsole anzeigen.

Die folgenden AWS Regionen unterstützen keine Kontrollen, die Teil des vom Security Hub Service verwalteten Standards sind: AWS Control Tower.

- Region Asien-Pazifik (Hongkong), ap-east-1
- Region Asien-Pazifik (Jakarta), ap-southeast-3
- Region Asien-Pazifik (Osaka), ap-northeast-3
- Region Europa (Mailand), eu-south-1
- Region Afrika (Kapstadt), af-south-1
- Region Naher Osten (Bahrain), me-south-1
- Israel (Tel Aviv), il-central-1
- Region Naher Osten (VAE), me-central-1
- Region Europa (Spanien), eu-south-2
- Region Asien-Pazifik (Hyderabad), ap-south-2
- Region Europa (Zürich), eu-central-2
- Region Asien-Pazifik (Melbourne), ap-southeast-4
- Kanada West (Calgary), ca-west-1

Die folgenden Systeme unterstützen AWS-Regionen keine proaktiven Kontrollen.

- Kanada West (Calgary)

Die folgende Tabelle zeigt proaktive Kontrollen, die in bestimmten Fällen nicht unterstützt werden AWS-Regionen.

Kennung des Steuerelements	Nicht unterstützte Regionen
`CT.REDSHIFT.PR.5`	ap-southeast-4, ap-south-2, ap-southeast-3, eu-central-2, eu-south-2, il-central-1, me-central-1
`CT.DAX.PR.2`	us-west-1
`CT.GLUE.PR.2`	Nicht unterstützt

Die folgende Tabelle zeigt AWS Control Tower Detective Controls, die in bestimmten Fällen nicht unterstützt werden AWS-Regionen.

Kontroll-ID	Nicht unterstützte Regionen
AWS-GR_AUTOSCALING_LAUNCH_CONFIG_PUBLIC_IP_DISABLED	ap-northeast-3, ap-southeast-3, il-central-1, ap-southeast-4, CA-West-1
AWS-GR_LAMBDA_FUNCTION_PUBLIC_ACCESS_PROHIBITED	eu-south-2
AWS-GR_EMR_MASTER_NO_PUBLIC_IP	ap-northeast-3, ap-southeast-3, Af-Süd-1, eu-south-1, IL-Zentral-1, me-central-1, eu-south-2, ap-south-2, eu-central-2, ap-southeast-4, CA-West-1
AWS-GR_EBS_SNAPSHOT_PUBLIC_RESTORABLE_CHECK	eu-south-2
AWS-GR_NO_UNRESTRICTED_ROUTE_TO_IGW	ap-northeast-3, ap-southeast-3, ap-south-2, eu-south-2, CA-West-1
AWS-GR_SAGEMAKER_NOTEBOOK_NO_DIRECT_INTERNET_ACCESS	ap-northeast-3, ap-southeast-3, Af-Süd-1, eu-south-1, IL-Zentral-1, me-central-1, eu-south-2, ap-south-2, eu-central-2, ap-southeast-4, CA-West-1
AWS-GR_EC2_INSTANCE_NO_PUBLIC_IP	ap-northeast-3
AWS-GR_EKS_ENDPOINT_NO_PUBLIC_ACCESS	ap-northeast-3, ap-southeast-3, af-south-1, eu-south-1, US-West-1, il-central-1, me-central-1, eu-south-2, ap-south-2, eu-central-2, ap-southeast-4, CA-West-1
AWS-GR_ELASTICSEARCH_IN_VPC_ONLY	ap-southeast-3, il-central-1, eu-south-2, ap-south-2, eu-central-2, ap-southeast-4, CA-West-1

Kontroll-ID	Nicht unterstützte Regionen
AWS-GR_RESTRICTED_SSH	af-south-1, ap-northeast-3, ap-south-2, ap-southeast-3, ap-southeast-4, eu-central-2, eu-south-1, eu-south-2, il-central-1, me-central-1
AWS-GR_DMS_REPLICATION_NOT_PUBLIC	af-south-1, ap-south-2 ap-southeast-3, ap-southeast-4, eu-central-2, eu-south-1, eu-south-2, il-central-1, me-central-1, ca-west-1
AWS-GR_RDS_SNAPSHOTS_PUBLIC_PROHIBITED	af-south-1, ap-southeast-4, eu-central-2, eu-south-1, eu-south-2, il-central-1
AWS-GR_SUBNET_AUTO_ASSIGN_PUBLIC_IP_DISABLED	ap-northeast-3
AWS-GR_ENCRYPTED_VOLUMES	af-south-1, ap-northeast-3, eu-south-1, il-central-1
AWS-GR_RESTRICTED_COMMON_PORTS	af-south-1, ap-northeast-3, eu-central-2, eu-south-1, eu-south-2, il-central-1, me-central-1
AWS-GR_IAM_USER_MFA_ENABLED	il-central-1, me-central-1, eu-soud-2, ap-south-2, eu-central-2, ap-southeast-4, ca-west-1
AWS-GR_MFA_ENABLED_FOR_IAM_CONSOLE_ACCESS	il-central-1, me-central-1, eu-soud-2, ap-south-2, eu-central-2, ap-southeast-4, ca-west-1
AWS-GR_SSM_DOCUMENT_NOT_PUBLIC	il-central-1, ca-west-1
AWS-GR_ROOT_ACCOUNT_MFA_ENABLED	il-central-1, me-central-1, ca-west-1
AWS-GR_S3_ACCOUNT_LEVEL_PUBLIC_ACCESS_BLOCKS_PERIODIC	il-central-1, eu-south-2, eu-central-2
AWS-GR_RDS_STORAGE_ENCRYPTED	eu-central-2, eu-south-2
AWS-GR_RDS_INSTANCE_PUBLIC_ACCESS_CHECK	ap-south-2, eu-south-2

Kontroll-ID	Nicht unterstützte Regionen
AWS-GR_REDSHIFT_CLUSTER_PUBLIC_ACCESS_CHECK	ap-south-2, ap-southeast-3, eu-south-2, CA-West-1
AWS-GR_EC2_VOLUME_INUSE_CHECK	ca-west-1
AWS-GR_EBS_OPTIMIZED_INSTANCE	ca-west-1

Regionen und Stapel setzen Grenzen

Wenn Sie planen, die Governance auf Organisationseinheiten mit einer großen Anzahl von Konten und einer großen Anzahl von auszudehnen AWS-Regionen, können Sie auf Einschränkungen stoßen, die durch AWS CloudFormation Stack-Sets für die Gesamtgröße einer Organisation entstehen. Sie können die Beschränkung mit der folgenden Formel abschätzen:

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

In der Regel gehen wir davon aus, dass die Anzahl der unterstützten Konten bei der Ausweitung der Verwaltung auf eine Organisationseinheit mit der Anzahl der verwalteten Regionen abnimmt.

Diese Einschränkung wird deutlich, wenn mehr als 15 Regionen, in denen AWS Control Tower verfügbar ist, aktiviert werden, wenn Sie die Governance auf eine Organisationseinheit ausweiten. Die Obergrenze für die Anzahl der Konten pro Organisationseinheit (OU) wird reduziert.

Wenn beispielsweise 22 Regionen aktiviert sind, liegt das Limit bei 220 Konten pro Organisationseinheit statt bei 300. Wenn Sie die Verwaltung auf Organisationseinheiten mit mehr als 220 Konten ausweiten möchten, müssen Sie die Anzahl der aktivierten Regionen reduzieren. Diese Reduzierung ist auf die Beschränkungen des Stack-Sets zurückzuführen.

Richtlinien:

- Mit 15 aktivierten Regionen werden Organisationseinheiten mit bis zu 300 Konten unterstützt
- Bei 22 aktivierten Regionen werden Organisationseinheiten mit bis zu 220 Konten unterstützt
- Bei 16 bis 21 aktivierten Regionen liegt die maximal unterstützte OU-Größe irgendwo im Bereich von 220-300 Konten
- Bei mehr als 23 aktivierten Regionen liegt die maximal unterstützte OU-Größe bei weniger als 220 Konten

Regionale Unterschiede bei der Funktionalität von AWS Control Tower

Es gibt gewisse Unterschiede im Verhalten von AWS Control Tower Across AWS-Regionen, da AWS Control Tower das Verhalten anderer AWS Services orchestriert. Beispielsweise:

- AWS Service Catalog ist nicht überall 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 Bereichen verfügbar.

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

- Ist es in Ihrer gewünschten Heimatregion AWS Service Catalog verfügbar?
- Sind die Steuerungen verfügbar, die Sie benötigen? Weitere Informationen finden Sie unter Einschränkungen der Steuerung.
- Ist IAM Identity Center in Ihrer gewünschten Heimatregion verfügbar?

Neu: Referenzhandbuch für AWS Control Tower Controls

Die Informationen zu Kontrollen in AWS Control Tower wurden in einen neuen Leitfaden, den AWS Control Tower Controls Reference Guide, 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, 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 zur AWS Sicherheit.
- IAM-Richtliniensimulator — Mit dem IAM-Richtliniensimulator können Sie IAM-basierte und ressourcenbasierte Richtlinien testen 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.

  Auf der Seite Aktivitäten finden Sie eine Übersichtstabelle der AWS Control Tower Tower-Ereignisse.

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). Im Vergleich dazu informiert Sie eine detektive Kontrolle anhand definierter AWS Config Regeln über verschiedene Ereignisse oder Zustände.

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.

Um Benutzern, die es wissen müssen, präventive Kontrollen aufzuzeigen

1. Melden Sie sich unter https://console.aws.amazon.com/controltower/ bei der AWS Control Tower Tower-Konsole an.
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 Ihrer Landing Zone von AWS Control Tower

Wenn Sie den Einrichtungsprozess durchlaufen, startet AWS Control Tower eine Schlüsselressource, die Ihrem Konto zugeordnet ist, die als Landing Zone bezeichnet wird und als Heimat für Ihre Organisationen und deren Konten dient.

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

Informationen zu einigen bewährten Methoden, die Sie bei der Planung und Einrichtung Ihrer Landing Zone befolgen sollten, finden Sie unter AWS Strategie für mehrere Konten für Ihre Landing Zone von AWS Control Tower.

Möglichkeiten zur Einrichtung von AWS Control Tower

Sie können eine Landing Zone von AWS Control Tower in einer vorhandenen Organisation einrichten oder zunächst eine neue Organisation erstellen, die Ihre Landing Zone von AWS Control Tower enthält.

- Starten von AWS Control Tower in einer vorhandenen Organisation: Dieser Abschnitt richtet sich an Kunden, die bereits AWS Organizations bereit sind, die Governance von AWS Control Tower einzuführen.
- Starten von AWS Control Tower in einer neuen Organisation: Dieser Abschnitt richtet sich an Kunden ohne bestehende AWS Organizations-, OUsKonten.

> **Note**
>
> Wenn Sie bereits über eine AWS Organizations Landing Zone verfügen, können Sie die AWS Control Tower-Governance von der vorhandenen Landing Zone auf einige oder alle Ihrer vorhandenen OUs und Konten innerhalb einer Organisation erweitern. Siehe Vorhandene Organisationen und Konten steuern.

Vergleichen der Funktionalität

Im Folgenden finden Sie einen kurzen Vergleich der Unterschiede zwischen dem Hinzufügen von AWS Control Tower zu einer bestehenden Organisation oder der Erweiterung der AWS Control Tower-Governance auf OUs 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 vorhandenen Organisation: Das Hinzufügen von AWS Control Tower zu einer vorhandenen Organisation ist etwas, das Sie in der AWS Konsole ausführen 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 danach eine Landing Zone hinzufügen.

Wenn Sie einer bestehenden Organisation eine Landing Zone hinzufügen, richtet AWS Control Tower eine parallele Struktur auf der AWS Organizations Ebene ein. Die OUs und Konten innerhalb Ihrer bestehenden Organisation werden dadurch nicht geändert.

Informationen zur Erweiterung der Governance: Die Erweiterung der Governance gilt für bestimmte OUs und Konten innerhalb einer einzelnen Organisation, die bereits bei AWS Control Tower registriert ist, was bedeutet, dass für diese Organisation bereits eine Landing Zone vorhanden ist. Die Erweiterung der Governance bedeutet, dass die Kontrollen von AWS Control Tower erweitert werden, sodass ihre Einschränkungen für die spezifischen OUs und Konten innerhalb dieser registrierten Organisation gelten. In diesem Fall starten Sie keine neue Landing Zone, sondern erweitern nur die aktuelle Landing Zone für Ihre Organisation.

> **Important**
>
> Besondere Überlegungen: 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, die bestimmen, ob AWS Control Tower Ihre aktuelle Bereitstellung der Landing Zone stören kann. Weitere Informationen finden Sie unter Walkthrough: Von ALZ zu AWS Control Tower wechseln. Informationen zum Verschieben von Konten von einer Landing Zone zu einer anderen finden Sie unter . Was ist, wenn das Konto die Voraussetzungen nicht erfüllt?

Starten von AWS Control Tower in einer vorhandenen Organisation

Durch die Einrichtung einer Landing Zone von AWS Control Tower in einer vorhandenen Organisation können Sie sofort parallel zu Ihrer vorhandenen AWS Organizations Umgebung arbeiten. Ihre anderen in OUs AWS Organizations sind 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 mithilfe des Verwaltungskontos Ihrer bestehenden Organisation als Verwaltungskonto. Es wird kein neues Verwaltungskonto benötigt. Sie können Ihre Landing Zone von AWS Control Tower über Ihr vorhandenes Verwaltungskonto starten.

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

Auswirkungen des Hinzufügens von AWS Control Tower zu Ihrer bestehenden Organisation

AWS Control Tower erstellt zwei Konten in Ihrer Organisation: ein Audit-Konto und ein Protokollierungskonto. Diese Konten führen Aufzeichnungen über die von Ihrem Team durchgeführten Aktionen in ihren individuellen Endbenutzerkonten. Die Audit -und Protokollarchivkonten werden in der Sicherheits-OU innerhalb Ihrer AWS Control Tower-Landing Zone angezeigt.

Wenn Sie Ihre Landing Zone einrichten, werden die von AWS Control Tower hinzugefügten Konten Teil Ihrer vorhandenen AWS Organizations, und daher werden sie Teil der Abrechnung für Ihre bestehende Organisation.

Zusammenfassung der Funktionen

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

- Sie ermöglicht eine einheitliche Abrechnung über die Gruppen Ihrer Organisation hinweg, da von AWS Control Tower hinzugefügte Konten Teil Ihrer bestehenden Organisation werden.
- Sie haben die Möglichkeit, alle Konten von einem Verwaltungskonto in Ihrer Organisationseinheit aus zu verwalten.
- Es vereinfacht die Anwendung und Durchsetzung von Kontrollen, die Sicherheit und Compliance für bestehende und neue Konten abdecken.

> **Important**
>
> Durch das Starten Ihrer Landing Zone von AWS Control Tower in einer vorhandenen AWS Organizations Organisation können Sie die AWS Control Tower-Governance von dieser Organisation auf andere OUs oder Konten erweitern, die nicht bei AWS Control Tower registriert sind.

Um AWS Control Tower in Ihrer vorhandenen 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 unter Kontrollieren von Organisationen und Konten mit AWS Control Tower.

Starten von AWS Control Tower in einer neuen Organisation

Wenn Sie AWS Control Tower noch nicht kennen und noch nicht mit gearbeitet haben AWS Organizations, sollten Sie am besten mit unserem Einrichtung Dokument beginnen.

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

AWS Strategie für mehrere Konten für Ihre Landing Zone von AWS Control Tower

AWS-Control-Tower-Kunden suchen häufig nach Anleitungen zur Einrichtung ihrer AWS Umgebung und Konten für beste Ergebnisse.AWS hat einen einheitlichen Satz von Empfehlungen erstellt, die als Strategie für mehrere Konten bezeichnet werden, damit Sie Ihre AWS Ressourcen optimal nutzen können, einschließlich Ihrer Landing Zone von AWS Control Tower.

Im Wesentlichen fungiert AWS Control Tower als Orchestrierungsebene, die mit anderen - AWS Services zusammenarbeitet und Sie bei der Implementierung der Empfehlungen für AWS mehrere Konten für AWS Konten und unterstützt AWS Organizations. Nachdem Ihre Landing Zone eingerichtet wurde, unterstützt AWS Control Tower Sie weiterhin bei der Verwaltung Ihrer Unternehmensrichtlinien und Sicherheitspraktiken über mehrere Konten und Workloads hinweg.

Die meisten Landing Zones entwickeln sich im Laufe der Zeit. Wenn die Anzahl der Organisationseinheiten (OUs) und Konten in Ihrer Landing Zone von AWS Control Tower zunimmt, können Sie Ihre AWS-Control-Tower-Bereitstellung so erweitern, dass Ihre Workloads effektiv organisiert werden können. Dieses Kapitel enthält vorgeschriebene Anleitungen zur Planung und Einrichtung Ihrer Landing Zone von AWS Control Tower im Einklang mit der AWS Strategie für mehrere Konten und zuren Erweiterung im Laufe der Zeit.

Allgemeine Informationen zu bewährten Methoden für Organisationseinheiten finden Sie unter Bewährte Methoden für Organisationseinheiten mit AWS Organizations.

AWS Strategie für mehrere Konten: Anleitung zu bewährten Methoden

AWS Bewährte Methoden für eine gut strukturierte Umgebung empfehlen, Ihre Ressourcen und Workloads in mehrere AWS Konten aufzuteilen. Sie können sich AWS Konten als isolierte Ressourcencontainer vorstellen: Sie bieten eine Kategorisierung der Workload sowie eine Reduzierung des Rotationsradius, wenn etwas schief geht.

Definition eines AWS Kontos

Ein - AWS Konto fungiert als Ressourcencontainer und Ressourcenisolationsgrenze.

> **Note**
>
> Ein - AWS Konto ist nicht mit einem Benutzerkonto identisch, das über Verbund oder AWS Identity and Access Management (IAM) eingerichtet wird.

Weitere Informationen zu - AWS Konten

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 Governance einer Workload-Umgebung.

Das AWS Konto ist der primäre Implementierungsmechanismus, um einen Ressourcencontainer für Ihre Workloads bereitzustellen. Wenn Ihre Umgebung gut strukturierte ist, können Sie mehrere AWS Konten effektiv verwalten und somit mehrere Workloads und Umgebungen verwalten.

AWS Control Tower richtet eine gut strukturierte Umgebung ein. Sie basiert auf - AWS Konten zusammen mit , die helfen AWS Organizations, Änderungen an Ihrer Umgebung zu regeln, die sich über mehrere Konten erstrecken können.

Definition einer gut strukturierten Umgebung

AWS definiert eine gut strukturierte Umgebung als 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 über mehrere Konten in Ihrer -Umgebung hinweg 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 AWS Konten
- Mehrere Organisationseinheiten (OUs)
- Eine gut geplante Struktur

Mehrere AWS-Konten verwenden

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

- Sicherheitskontrollen – Anwendungen haben unterschiedliche Sicherheitsprofile, daher erfordern sie unterschiedliche Kontrollrichtlinien und Mechanismen. Beispielsweise ist es weitaus einfacher, mit einem Prüfer zu sprechen und auf ein einzelnes Konto zu verweisen, das den Workload der Zahlungskartenbranche (PCI) hostet.
- Isolation – Ein Konto ist eine Einheit des Sicherheitsschutzes. Mögliche Risiken und Sicherheitsbedrohungen können in einem Konto enthalten sein, ohne andere zu beeinträchtigen. Daher erfordern Sicherheitsanforderungen möglicherweise, dass Sie Konten voneinander isolieren. Sie können beispielsweise 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 es bei der Verwendung desselben Kontos der Fall ist.
- 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 Isolation trägt dazu bei, die unbefugte Offenlegung hochprivater Daten zu verhindern. Beispielsweise unterstützt die Datenisolierung die Einhaltung der Datenschutz-Richtlinie (GDPR).

- Geschäftsprozess – Geschäftsbereiche oder Produkte haben oft völlig unterschiedliche Zwecke und Prozesse. Einzelne Konten können eingerichtet werden, um geschäftsspezifische Anforderungen zu erfüllen.
- Fakturierung – Ein Konto ist die einzige Möglichkeit, Elemente auf Fakturierungsebene zu trennen, einschließlich Übertragungskosten usw. Die Strategie für mehrere Konten hilft dabei, separate abrechenbare Elemente über Geschäftsbereiche, Funktionsteams oder einzelne Benutzer hinweg zu erstellen.
- Kontingentzuweisung – AWS Kontingente werden pro Konto eingerichtet. Durch die Trennung von Workloads in verschiedene Konten erhält jedes Konto (z. B. ein Projekt) ein definiertes, individuelles Kontingent.

Mehrere Organisationseinheiten verwenden

AWS Control Tower und andere Frameworks zur Kontoorchestrierung können Änderungen vornehmen, die Kontogrenzen überschreiten. Daher berücksichtigen die AWS bewährten Methoden kontoübergreifende Änderungen, die möglicherweise eine Umgebung beschädigen oder ihre Sicherheit untergraben können. In einigen Fällen können sich Änderungen über Richtlinien hinaus auf die gesamte Umgebung auswirken. Daher empfehlen wir Ihnen, mindestens zwei obligatorische Konten einzurichten: Produktion und Staging.

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

Unsere Empfehlung besteht darin, mindestens eine Vorproduktionsumgebung (oder Staging) zu erstellen, die sich von Ihrer Produktionsumgebung unterscheidet – mit unterschiedlichen Kontrollen und Richtlinien. Die Produktions- und Staging-Umgebungen können als separate OUs erstellt und verwaltet und als separate Konten abgerechnet werden. Darüber hinaus können Sie eine Sandbox-OU für Codetests einrichten.

Verwenden Sie eine gut geplante Struktur für OUs in Ihrer Landing Zone

AWS Control Tower richtet automatisch einige OUs für Sie ein. Wenn sich Ihre Workloads und Anforderungen im Laufe der Zeit erweitern, können Sie die ursprüngliche Konfiguration der Landing Zone an Ihre Anforderungen anpassen.

> **Note**
>
> Die in den Beispielen angegebenen Namen folgen den vorgeschlagenen AWS Namenskonventionen für die Einrichtung einer AWS Umgebung mit mehreren Konten. Sie können Ihre OUs umbenennen, nachdem Sie Ihre Landing Zone eingerichtet haben, indem Sie auf der Detailseite der Organisationseinheit die Option Bearbeiten auswählen.

Empfehlungen

Nachdem AWS Control Tower die erste erforderliche Organisationseinheit für Sie eingerichtet hat – die Sicherheitsorganisationseinheit – empfehlen wir, einige zusätzliche OUs in Ihrer Landing Zone zu erstellen.

Wir empfehlen, dass Sie AWS Control Tower erlauben, mindestens eine zusätzliche Organisationseinheit zu erstellen, die als Sandbox-Organisationseinheit bezeichnet wird. Diese Organisationseinheit ist für Ihre Softwareentwicklungsumgebungen bestimmt. AWS Control Tower kann die Sandbox-OU während der Erstellung der Landing Zone für Sie einrichten, wenn Sie sie auswählen.

Zwei empfohlene andere OUs, die Sie selbst einrichten können: die Infrastruktur-Organisationseinheit, um Ihre freigegebenen Services und Netzwerkkonten zu enthalten, und eine Organisationseinheit, um Ihre Produktions-Workloads zu enthalten, die als Workloads-Organisationseinheit bezeichnet wird. Sie können zusätzliche OUs in Ihrer Landing Zone über die AWS Control Tower-Konsole auf der Seite Organisationseinheiten hinzufügen.

Empfohlene OUs neben den automatisch eingerichteten Organisationseinheiten

- Infrastruktur-OU – Enthält Ihre freigegebenen Services und Netzwerkkonten.

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

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

> **Note**
>
> AWS Control Tower empfiehlt, die Sandbox-OU einzurichten, 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 Produktionsstarter-Organisation mit AWS Control Tower.

Beispiel für AWS Control Tower mit einer vollständigen Organisationseinheitsstruktur mit mehreren 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-Umgebung erstellen, die den Richtlinien für Strategien mit AWS mehreren Konten entspricht.

Sie können auch eine einfachere, flache Organisationseinheitsstruktur erstellen, die gut funktioniert und den Richtlinien für AWS mehrere Konten entspricht. Nur weil Sie eine hierarchische Organisationseinheitsstruktur erstellen können, bedeutet dies nicht, dass Sie dies tun müssen.

- Ein Diagramm, das einen Beispielsatz von OUs in einer erweiterten, flachen AWS Control Tower-Umgebung mit Anleitungen für AWS mehrere Konten zeigt, finden Sie unter Beispiel: Workloads in einer flachen Organisationseinheitenstruktur.
- Weitere Informationen zur Funktionsweise von AWS Control Tower mit verschachtelten OU-Strukturen finden Sie unter Verschachtelte Organisationseinheiten im AWS Control Tower.
- Weitere Informationen darüber, wie AWS Control Tower den AWS Anleitungen entspricht, finden Sie im AWS Whitepaper Organisieren Ihrer AWS Umgebung mit mehreren Konten.

Das Diagramm auf der verknüpften Seite zeigt, dass mehr grundlegende OUs und mehr zusätzliche OUs erstellt wurden. Diese OUs erfüllen die zusätzlichen Anforderungen einer größeren Bereitstellung.

In der Spalte Grundlegende OUs wurden der grundlegenden Struktur zwei OUs hinzugefügt:

- Security_Prod OU – Bietet einen schreibgeschützten Bereich für Sicherheitsrichtlinien sowie einen Sicherheitsüberwachungsbereich für Break-Glass.
- Infrastruktur-OU – Möglicherweise möchten Sie die Infrastruktur-OU, die zuvor empfohlen wurde, in zwei OUs aufteilen: Infrastructure_Test (für die Vorproduktionsinfrastruktur) und Infrastructure_Prod (für die Produktionsinfrastruktur).

Im Bereich Zusätzliche OUs wurden der Grundstruktur weitere OUs hinzugefügt. Im Folgenden finden Sie die nächsten empfohlenen OUs, die Sie erstellen sollten, wenn Ihre Umgebung wächst:

- Workloads-OU – Die zuvor empfohlene Workloads-OU wurde in zwei OUs unterteilt: Workloads_Test (für Workloads vor der Produktion) und Workloads_Prod (für Produktions-Workloads).
- PolicyStaging Organisationseinheit – Ermöglicht es Systemadministratoren, ihre Änderungen an Kontrollen und Richtlinien zu testen, bevor sie vollständig angewendet werden.
- Unterbrochene Organisationseinheit – Bietet einen Speicherort für Konten, die möglicherweise vorübergehend deaktiviert wurden.

Informationen zum Root

Der Root ist keine Organisationseinheit. Es ist ein Container für das Verwaltungskonto und für alle OUs und Konten in Ihrer Organisation. Konzeptionell enthält der Root alle OUs . Es kann nicht gelöscht werden. Sie können registrierte Konten nicht auf Root-Ebene in AWS Control Tower regeln. Stattdessen sollten Sie registrierte Konten innerhalb Ihrer OUsregeln. Ein hilfreiches Diagramm finden Sie in der AWS Organizations Dokumentation zu .

Administrative Tipps für die Einrichtung der 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 AWS Control Tower unterstützt Tagging für aktivierte Kontrollen.
- Wir empfehlen, die Multi-Faktor-Authentifizierung (MFA) für jedes Konto zu aktivieren, das AWS Control Tower verwaltet.

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 ist nicht identisch mit 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.

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 in 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:

  - Behalten Sie einen aktiven AWS Config Rekorder bei. Wenn Sie Ihren Config-Recorder löschen, kann Detective Controls Abweichungen nicht erkennen und melden. Ressourcen, die nicht konform sind, können aufgrund unzureichender Informationen als konform gemeldet werden.
  - 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 sich jedoch auf unvorhersehbare Weise auf die Funktionalität von AWS Control Tower auswirken, 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 300 Konten zu verwenden, sodass Sie diese Konten mit der Funktion „Organisationseinheit erneut registrieren“ 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 Organisationseinheit auf etwa 150 zu beschränken, obwohl die Obergrenze bei 300 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 benötigt eine Organisationseinheit mit 150 Konten etwa 2 Stunden, um sich zu registrieren und die Kontrollen zu aktivieren, und etwa 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 Aktualisierung und Verschiebung von Accountfactory-Konten mit AWS Control Tower oder mit AWS Service Catalog.
- Um einen zu schließen AWS-Konto.
- Weitere Informationen zu Aktionen, für die Root-Benutzeranmeldedaten erforderlich sind, finden Sie im AWS Account Management 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 ein Benutzer mit den entsprechenden IAM-Berechtigungen sein. .

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.

AWS Organizations Anleitung

- 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 Verfahren für Mitgliedskonten
- Verwenden Sie es nicht AWS Organizations , um Service Control Policies (SCPs) zu aktualisieren, die an eine OU angehängt sind, die bei AWS Control Tower registriert ist. Dies könnte dazu führen, dass die Kontrollen in einen unbekannten Zustand übergehen, sodass Sie Ihre landing zone zurücksetzen oder Ihre Organisationseinheit erneut im AWS Control Tower registrieren müssen. Stattdessen können Sie neue SCPs erstellen und diese an die OUs anhängen, anstatt die von AWS Control Tower erstellten SCPs zu bearbeiten.

- 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 Governance-Abweichungen.
- 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 handhabt 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 sich jedoch auf unvorhersehbare Weise auf die Funktionalität von AWS Control Tower auswirken, 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

> **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.

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.

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 AWS IAM Identity Center in AWS Control Tower einzustellen oder mit der Nutzung von AWS IAM Identity Center zu beginnen

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 Prüfungen vor dem Start 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

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 Fehler: Keine Startpfade gefunden im Abschnitt zur Fehlerbehebung im AWS Control Tower Tower-Benutzerhandbuch.

> **Note**
>
> Es können bis zu fünf Konten gleichzeitig bereitgestellt werden.

Hinweise zum Abonnieren von SNS-Themen

- 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. Beispielsweise:

```
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.

KI-basierte Services und AWS Control Tower

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

Diese SCP-Richtlinien zur KI-Deaktivierung 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	Beschreibung
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
2.5	18.11.2020	Landezone Version 2.5

Version	Datum der Veröffentlichung	Beschreibung
2.4	Keine	None
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 Update - 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.

Informationen zu Aktualisierungen

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 aktualisiert werden, indem Sie OU erneut registrieren wählen, oder mithilfe eines automatisierten Skripting-Ansatzes, der in einem späteren Abschnitt dieser Seite beschrieben wird.
- Vollständige Aktualisierung: Eine vollständige Aktualisierung beinhaltet die Aktualisierung Ihrer Landing Zone, gefolgt von der Aktualisierung aller angemeldeten Konten in Ihrer registrierten OU. Bei einer neuen Version von AWS Control Tower wie 2.9, 3.0 usw. sind vollständige Updates erforderlich.

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

Aktualisieren Ihrer 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.

Manuelle Updates

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

Um deine landing zone manuell 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 300 Konten befolgt werden).
4. Wählen Sie im linken Navigationsbereich Organisation aus.
5. Gehen Sie wie unter beschrieben vor, um jedes Konto zu aktualisierenAktualisieren Sie das Konto in der Konsole.

> Optional können Sie die Organisationseinheit erneut registrieren, um Konten zu aktualisieren
>
> Für registrierte AWS Control Tower Tower-Organisationseinheiten mit weniger als 300 Konten können Sie auf der OU-Seite im Dashboard die Option OU erneut registrieren auswählen, um die Konten in dieser OU zu aktualisieren.

Beheben Sie Abweichungen mit Reset und erneuter Registrierung

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 die meisten Arten von Drift zu beheben, wählen Sie auf der Seite mit den Einstellungen für die Landezone die Option Zurücksetzen. Außerdem können Sie einige Arten von Abweichungen beheben, indem Sie eine Organisationseinheit erneut registrieren. Weitere Informationen zu Arten von Abweichungen und deren Behebung finden Sie unter Arten von Governance-Abweichungen undAbweichungen 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 Landezone-Version zu beheben, sind zwei Verhaltensweisen möglich.

- Wenn Sie die neueste Landing Zone-Version verwenden, werden Ihre Drifted landing zone Zone-Ressourcen auf die gespeicherte AWS Control Tower Tower-Konfiguration zurückgesetzt, wenn Sie Zurücksetzen und dann Bestätigen wählen. Die Landezone-Version bleibt gleich.
- Wenn Sie nicht die neueste Version verwenden, müssen Sie Update wählen. Die landing zone wurde auf die neueste Landezonenversion aktualisiert. Die Drift wird im Rahmen dieses Prozesses behoben.

Konten mithilfe von Automatisierung bereitstellen und aktualisieren

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 Walkthrough: Automatisieren der Kontobereitstellung in AWS Control Tower über 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 von AWS CloudShell für die Arbeit mit AWS Control Tower.
- Automatisieren Sie Aufgaben in AWS Control Tower .

Automatisieren Sie Aufgaben in AWS Control Tower

Viele Kunden ziehen es vor, Aufgaben in AWS Control Tower zu automatisieren, wie Kontobereitstellung, Kontrollzuweisung und Prüfung. Sie können diese automatisierten Aktionen mit Aufrufen einrichten:

- AWS Service Catalog APIs
- AWS Organizations APIs
- AWS Control Tower Tower-APIs
- die AWS CLI

Die Ähnliche Informationen Seite enthält Links zu vielen ausgezeichneten 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 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 Tower-API automatisieren. Einzelheiten finden Sie in der AWS Control Tower API-Referenz.

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

Automatisieren von Aufgaben in der landing zone

Die AWS Control Tower Landing Zone-APIs helfen Ihnen dabei, bestimmte Aufgaben im Zusammenhang mit Ihrer landing zone zu automatisieren. Einzelheiten finden Sie in der AWS Control Tower API-Referenz.

Automatisierung der OU-Registrierung

Die AWS Control Tower Tower-Baseline-APIs helfen Ihnen dabei, bestimmte Aufgaben zu automatisieren, z. B. die Registrierung einer Organisationseinheit. Einzelheiten finden Sie in der AWS Control Tower API-Referenz.

Automatisierte Kontoschließung

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

Automatisierte Kontobereitstellung und -aktualisierung

AWS Control Tower Account Factory Customization (AFC) unterstützt Sie bei der Erstellung von Konten über die AWS Control Tower Tower-Konsole mit benutzerdefinierten AWS CloudFormation Vorlagen, die wir als Blueprints bezeichnen. Dieser Prozess ist insofern automatisiert, als Sie nach der Einrichtung eines einzigen Blueprints wiederholt neue Konten erstellen und Konten aktualisieren können, ohne 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 Bereitstellen von Konten mit AWS Control Tower Account Factory for Terraform (AFT) .

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 und Service Control Policies (SCPs) 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.

Weitere Informationen finden Sie unter Konten per Skript aktualisieren.

Programmatische Prüfung von Konten

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

Automatisieren anderer Aufgaben

Informationen dazu, wie Sie bestimmte AWS Control Tower Tower-Servicekontingenten mit einer automatisierten Anforderungsmethode erhöhen können, finden Sie in diesem Video: Automate Service Limit Increases.

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

Auf der Website sind zwei Open-Source-Beispiele verfügbar GitHub , die Ihnen bei bestimmten Automatisierungsaufgaben im Zusammenhang mit der Sicherheit helfen sollen.

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

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

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

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

Verwenden von AWS CloudShell für die Arbeit mit AWS Control Tower

AWS CloudShell ist ein - AWS Service, der die Arbeit in der AWS -CLI erleichtert – es ist eine browserbasierte, vorauthentifizierte Shell, die Sie direkt über die starten können AWS Management Console. Es ist nicht erforderlich, Befehlszeilen-Tools herunterzuladen oder zu installieren. Sie können AWS CLI Befehle für AWS Control Tower und andere - AWS Services von Ihrer bevorzugten Shell (Bash PowerShell oder Z-Shell) aus ausführen.

Wenn Sie über die starten AWS CloudShellAWS Management Console, sind die AWS Anmeldeinformationen, mit denen Sie sich bei der Konsole angemeldet haben, in einer neuen

Shell-Sitzung verfügbar. Sie können die Eingabe Ihrer Konfigurationsanmeldeinformationen überspringen, wenn Sie mit AWS Control Tower und anderen - AWS Services interagieren, und Sie verwenden AWS CLI Version 2, die in der Rechenumgebung der Shell vorinstalliert ist. Sie sind mit vorauthentifiziert AWS CloudShell.

Abrufen von IAM-Berechtigungen für AWS CloudShell

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

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

- `AWSCloudShellFullAccess`: Gewährt die Berechtigung zur Verwendung AWS CloudShell von mit vollem Zugriff auf alle Funktionen.

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

> **Note**
>
> Ihre IAM-Identität erfordert auch eine Richtlinie, die die Berechtigung zum Aufrufen von erteilt AWS Control Tower. Weitere Informationen finden Sie unter Erforderliche Berechtigungen für die Verwendung der AWS Control Tower Konsole.

Interaktion mit AWS Control Tower mithilfe von AWS CloudShell

Nachdem Sie AWS CloudShell über die gestartet haben AWS Management Console, können Sie sofort mit der Interaktion mit AWS Control Tower über die Befehlszeilenschnittstelle beginnen. - AWS CLI Befehle funktionieren standardmäßig 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 vor Aufrufen keine Anmeldeinformationen konfigurieren müssen.

Starten AWS CloudShell

- In der können Sie starten AWS Management Console, CloudShell indem Sie die folgenden Optionen auswählen, die auf der Navigationsleiste verfügbar sind:

  - Wählen Sie das CloudShell Symbol aus.
  - Geben Sie „cloudshell“ in das Suchfeld ein und wählen Sie dann die CloudShell Option aus.

  Nachdem Sie nun gestartet haben CloudShell, können Sie alle AWS CLI Befehle eingeben, die Sie für die Arbeit mit benötigen AWS Control Tower. Sie können beispielsweise Ihren AWS Config Status überprüfen.

Verwenden von AWS CloudShell zur Unterstützung bei der Einrichtung von AWS Control Tower

Bevor Sie diese Verfahren ausführen, müssen Sie bei der AWS Management Console in der Heimatregion für Ihre Landing Zone angemeldet sein, und Sie müssen 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 in verwenden AWS CloudShell , um den Status Ihres Konfigurations-Recorders und Übermittlungskanals zu bestimmen, bevor Sie mit der Konfiguration Ihrer AWS Control Tower Landing Zone beginnen.

   Überprüfen Ihres AWS Config Status

   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"`

2. Wenn Sie über einen vorhandenen AWS Config Recorder oder Übermittlungskanal verfügen, den Sie löschen müssen, bevor Sie Ihre AWS Control Tower Landing Zone einrichten, können Sie hier einige Befehle eingeben:

   Verwalten bereits vorhandener AWS Config Ressourcen

   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 in einen inkonsistenten Zustand wechselt.

   Weitere Informationen finden Sie in der AWS Config-Dokumentation.

   - Verwalten von Configuration Recorder (AWS CLI)
   - Verwalten des Übermittlungskanals

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

   Aktivieren oder Deaktivieren des vertrauenswürdigen Servicezugriffs

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

Erstellen eines Amazon S3-Buckets mit AWS CloudShell

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

1. Um einen Bucket in einer angegebenen 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 in Kleinbuchstaben), wird der folgende Fehler angezeigt: Beim Aufrufen der CreateBucket Operation ist ein Fehler (InvalidBucketName) aufgetreten: Der angegebene Bucket ist ungültig.

2. Um eine Datei hochzuladen und sie als Objekt zum soeben erstellten Bucket hinzuzufügen, rufen Sie die -PutObjectMethode 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 vom Service ähnlich der folgenden Ausgabe an:

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

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

AWS Control Tower Ressourcen erstellen 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 gewünschten AWS Ressourcen beschreibt, z. B. `AWS::ControlTower::EnabledControl` für Steuerelemente. AWS CloudFormation stellt diese Ressourcen für Sie bereit und konfiguriert sie.

Wenn Sie Ihre Vorlage verwenden AWS CloudFormation, können Sie sie 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 Regionen bereit.

AWS Control Tower und AWS CloudFormation Vorlagen

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

AWS Control Tower unterstützt das Erstellen `AWS::ControlTower::EnabledControl` (Steuern von Ressourcen), `AWS::ControlTower::LandingZone` (Landezonen) und `AWS::ControlTower::EnabledBaseline` (Baselines) in. AWS CloudFormationWeitere Informationen, einschließlich Beispielen für JSON- und YAML-Vorlagen für diese Ressourcentypen, finden Sie AWS Control Towerim AWS CloudFormation Benutzerhandbuch.

> **Note**
>
> Das Limit für `EnableControl` und `DisableControl` Aktualisierungen AWS Control Tower liegt bei 100 gleichzeitigen Vorgängen, wobei bis zu 20 dieser Vorgänge proaktive Kontrollen betreffen.

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

Erfahren Sie mehr über AWS CloudFormation

Weitere Informationen AWS CloudFormation dazu finden Sie in den folgenden Ressourcen:

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

Passen Sie Ihre AWS Control Tower Tower-Landezone an

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

Mit der Funktion „Anpassungen für AWS Control Tower“ können Sie beispielsweise umfassendere Anpassungen Ihrer landing zone vornehmen. Dabei handelt es sich um ein Framework für Anpassungen GitOps im Stil von AWS, das mit AWS CloudFormation Vorlagen und AWS Control Tower Tower-Lifecycle-Ereignissen arbeitet.

Anpassen über die AWS Control Tower Tower-Konsole

Folgen Sie den in der AWS Control Tower Tower-Konsole angegebenen Schritten, um diese Anpassungen an Ihrer landing zone vorzunehmen.

Wählen Sie bei der Einrichtung benutzerdefinierte Namen aus

- Sie können während der Einrichtung die Namen Ihrer Organisationseinheiten auf oberster Ebene auswählen. Sie können Ihre Organisationseinheiten jederzeit über die 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 gemeinsamen 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 durch das Umbenennen einer Organisationseinheit in AWS Organizations das entsprechende bereitgestellte Produkt in Account Factory nicht aktualisiert wird. Um das bereitgestellte Produkt automatisch zu aktualisieren (und Abweichungen zu vermeiden), müssen Sie den OU-Vorgang über AWS Control Tower durchführen, einschließlich der Erstellung, Löschung oder erneuten Registrierung einer OU.

Wählen Sie Regionen aus AWS

- Sie können Ihre landing zone anpassen, indem Sie bestimmte AWS Regionen für die Verwaltung auswählen. Folgen Sie den Schritten in der AWS Control Tower Tower-Konsole.
- Sie können AWS Regionen für die Verwaltung auswählen und deren Auswahl aufheben, wenn Sie Ihre landing zone aktualisieren.
- Sie können die Option „Region verweigern“ auf „Aktiviert“ oder „Nicht aktiviert“ setzen und den Benutzerzugriff auf die meisten AWS Dienste in Regionen ohne Regierung kontrollieren. AWS

Informationen darüber, AWS-Regionen wo cFCT Bereitstellungsbeschränkungen hat, finden Sie unter. Einschränkungen der Kontrolle

Passen Sie es an, indem Sie optionale Steuerelemente hinzufügen

- Dringend empfohlene und optionale Kontrollen sind optional, was bedeutet, dass Sie den Grad der Durchsetzung für Ihre landing zone anpassen können, indem Sie auswählen, welche aktiviert werden sollen. Optionale Kontrollen sind standardmäßig nicht aktiviert.
- Mit den optionalen Steuerelementen zur Datenresidenz können Sie die Regionen anpassen, in denen Sie Ihre Daten speichern, und den Zugriff darauf gewähren.
- Mit den optionalen Kontrollen, die Teil des integrierten Security Hub Hub-Standards sind, können Sie Ihre AWS Control Tower Tower-Umgebung scannen, um nach Sicherheitsrisiken zu suchen.
- Mit den optionalen proaktiven Kontrollen können Sie Ihre AWS CloudFormation Ressourcen überprüfen, bevor sie bereitgestellt werden, um sicherzustellen, dass die neuen Ressourcen den Kontrollzielen Ihrer Umgebung entsprechen.

Passen Sie Ihre Trails individuell an AWS CloudTrail

- Wenn Sie Ihre landing zone auf Version 3.0 oder höher aktualisieren, können Sie wählen, ob Sie die von AWS Control Tower verwalteten CloudTrail Trails auf Organisationsebene aktivieren oder deaktivieren möchten. Sie können diese Auswahl jederzeit ändern, wenn Sie Ihre landing zone aktualisieren. AWS Control Tower erstellt einen Trail auf Organisationsebene in Ihrem Verwaltungskonto, und dieser Trail 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.

Erstellen Sie benutzerdefinierte Mitgliedskonten in der Konsole

- Über die AWS Control Tower Tower-Konsole können Sie benutzerdefinierte AWS Control Tower Tower-Mitgliedskonten erstellen und bestehende Mitgliedskonten 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 Tower-Konsole

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

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

  AFT wird mit einem Terraform-Modul bereitgestellt, das im AFT-Repository verfügbar ist.
- Mit Customizations for AWS Control Tower (cFCT), einem Funktionspaket, das auf AWS CloudFormation Vorlagen und Service Control Policies (SCPs) aufbaut, können Sie Ihre AWS Control Tower-Landezone individuell anpassen. 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.

Vorteile von Anpassungen für AWS Control Tower (cFCT)

Das Funktionspaket, das wir als Customizations for AWS Control Tower (cFCT) bezeichnen, hilft Ihnen dabei, umfangreichere Anpassungen für Ihre landing zone vorzunehmen, als Sie es in der AWS Control Tower-Konsole tun können. Es bietet einen automatisierten Prozess GitOps im A-Stil. Sie können Ihre landing zone an Ihre Geschäftsanforderungen anpassen.

Dieser infrastructure-as-codeAnpassungsprozess integriert AWS CloudFormation Vorlagen mit AWS Service Control Policies (SCPs) und AWS Control Tower Tower-Lifecycle-Ereignissen, sodass Ihre Ressourcenbereitstellungen mit Ihrer landing zone synchronisiert bleiben. Wenn Sie beispielsweise ein neues Konto bei Account Factory erstellen, können die mit dem Konto und der Organisationseinheit 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 Organisationseinheiten in Ihrer landing zone, indem von Ihnen angegebene Ressourcen bereitgestellt werden.

Vorteile

- Erweitern Sie eine maßgeschneiderte und sichere AWS Umgebung — Sie können Ihre AWS Control Tower 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 Tower-Landing landing zone an Ihre Geschäftsanforderungen anpassen, indem Sie die AWS CloudFormation Vorlagen und Richtlinien zur Servicekontrolle verwenden, die Ihre politischen Absichten zum Ausdruck bringen.
- Weitere Automatisierung mit Lebenszyklusereignissen von AWS Control Tower — 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 Netzwerkanwendungsfall 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 zu CfCT und Amazon GuardDuty ist GitHub im `aws-samples`Repository verfügbar.
- Weitere 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 den AWS Prescriptive Guidance.

Übersicht über Anpassungen für AWS Control Tower (CfCT)

Anpassungen für AWS Control Tower (CfCT) helfen Ihnen dabei, Ihre Landing Zone von AWS Control Tower anzupassen und auf die AWS bewährten Methoden abgestimmt zu bleiben. Anpassungen werden mit AWS CloudFormation Vorlagen und Service-Kontrollrichtlinien (SCPs) implementiert.

Diese CfCT-Funktion ist in Lebenszyklusereignisse von AWS Control Tower integriert, sodass Ihre Ressourcenbereitstellungen mit Ihrer Landing Zone synchronisiert bleiben. Wenn beispielsweise ein neues Konto über die 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) in Ihrer Organisation bereitstellen.

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

Der folgende Abschnitt enthält Überlegungen zur Architektur und zu Konfigurationsschritten für die Bereitstellung von Anpassungen für AWS Control Tower (CfCT). Sie enthält einen Link zu der AWS CloudFormation Vorlage, die die erforderlichen AWS Services im Einklang mit AWS bewährten Methoden für Sicherheit und Verfügbarkeit startet, konfiguriert und ausführt.

Dieses Thema richtet sich an IT-Infrastrukturarchitekten und Entwickler, die über praktische Erfahrungen mit Architekturen in der AWS -Cloud verfügen.

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

Übersicht über die Architektur

Durch die Bereitstellung von CfCT wird die folgende Umgebung in der AWS Cloud erstellt.

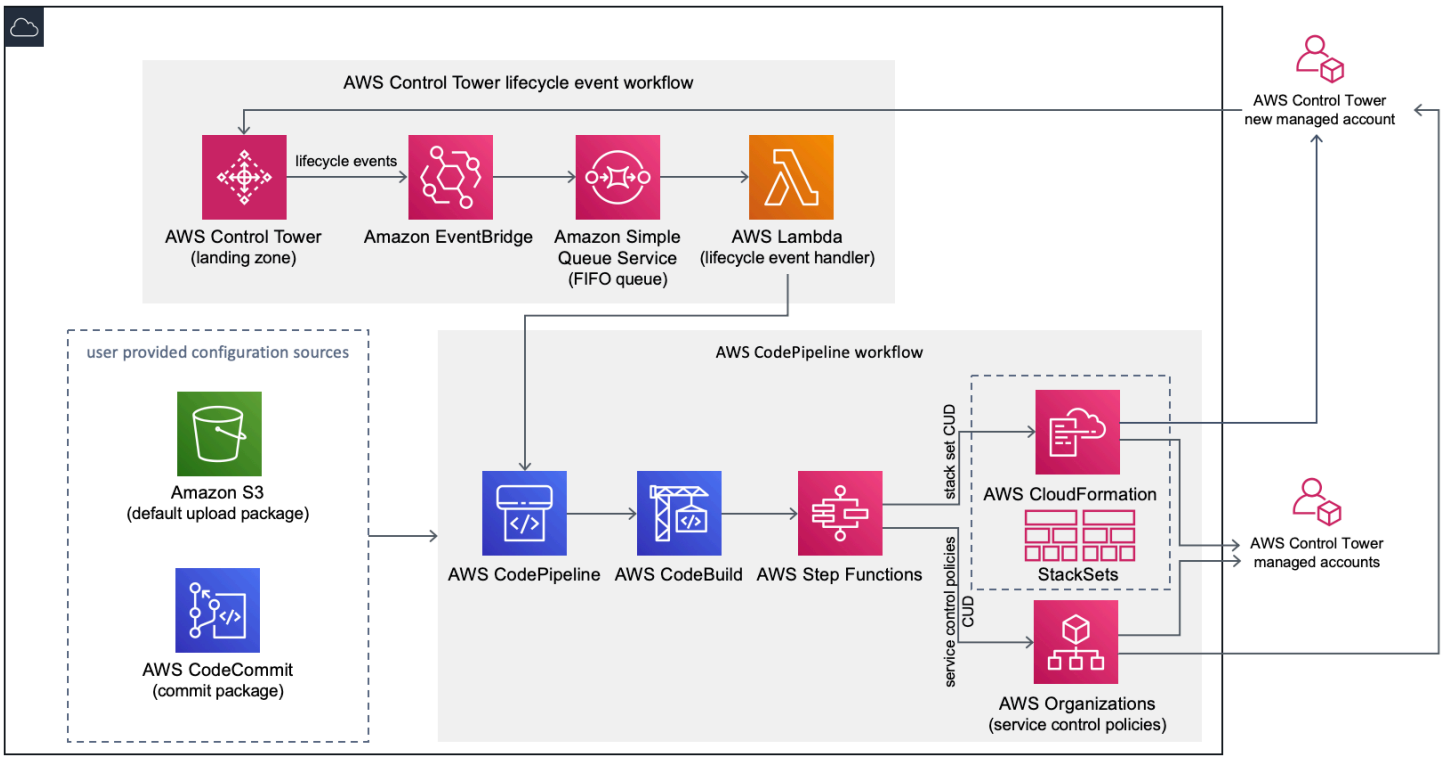


Abbildung 1: Anpassungen für die AWS Control Tower-Architektur

CfCT enthält eine - AWS CloudFormation Vorlage, die Sie in Ihrem AWS Control Tower-Verwaltungskonto bereitstellen. Die Vorlage startet alle Komponenten, die zum Erstellen der Workflows erforderlich sind, sodass Sie Ihre Landing Zone von AWS Control Tower anpassen können.

> **Hinweis**
>
> CfCT muss in der Heimatregion von AWS Control Tower und im Verwaltungskonto von AWS Control Tower bereitgestellt werden, da dort Ihre Landing Zone von AWS Control Tower bereitgestellt wird. Informationen zum Einrichten einer Landing Zone von AWS Control Tower finden Sie unter Erste Schritte.

Wenn Sie CfCT bereitstellen, werden die benutzerdefinierten Ressourcen mithilfe von Amazon Simple Storage Service (Amazon S3) verpackt und in die Code-Pipeline-Quelle hochgeladen. Der Upload-Prozess ruft automatisch den Zustandsautomaten für Service-Kontrollrichtlinien (SCPs) und den AWS CloudFormation StackSets Zustandsautomaten auf, um die SCPs auf Organisationseinheitsebene bereitzustellen oder Stack-Instances auf Organisationseinheits- oder Kontoebene bereitzustellen.

> **Hinweis**
>
> Standardmäßig erstellt CfCT einen Amazon S3-Bucket zum Speichern der Pipeline-Quelle, Sie können jedoch den Speicherort in ein -AWS CodeCommitRepository ändern. Weitere Informationen finden Sie unter Einrichten von Amazon S3 als Konfigurationsquelle.

CfCT stellt zwei Workflows bereit:

- einen -AWS CodePipelineWorkflow
- und ein AWS Control Tower-Lebenszyklusereignis-Workflow.

Der AWS CodePipeline Workflow

Der AWS CodePipeline Workflow konfiguriert AWS CodePipeline, AWS CodeBuild Projekte und , AWS Step Functions die die Verwaltung von AWS CloudFormation StackSets und SCPs in Ihrer Organisation orchestrieren.

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

- Build-Phase – validiert den Inhalt des Konfigurationspakets mit AWS CodeBuild.
- SCP-Stufe – ruft den Zustandsautomaten der Service-Kontrollrichtlinie auf, der die AWS Organizations -API aufruft, um SCPs zu erstellen.
- AWS CloudFormation Stage – ruft den Stack-Set-Zustandsautomaten auf, um die in der Liste der Konten oder OUs angegebenen Ressourcen bereitzustellen, die Sie in der Manifestdatei angegeben haben.

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

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

Der Lebenszyklusereignis-Workflow 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 Amazon EventBridge-Ereignisregel, einer Amazon Simple Queue Service (Amazon SQS) First-In First-Out (FIFO)-Warteschlange und einer -AWS LambdaFunktion besteht.

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

Kosten

Die Kosten für die Ausführung von CfCT hängen von der Anzahl der AWS CodePipeline Ausführungen, der Dauer der AWS CodeBuild Ausführungen, der Anzahl und Dauer der AWS Lambda Funktionen sowie der Anzahl der veröffentlichten Amazon- EventBridge Ereignisse ab. Wenn Sie beispielsweise 100 Builds in einem Monat mit build.general1.small ausführen, wobei jeder Build fünf Minuten lang ausgeführt wird, betragen die ungefähren Kosten für die Ausführung von CfCT 3,00 USD pro Monat. Ausführliche Informationen finden Sie auf der Webseite -Preise für jeden AWS Service, den Sie ausführen.

Der Amazon Simple Storage Service (Amazon S3)-Bucket und die AWS CodeCommit Git-basierten Repository-Ressourcen werden nach dem Löschen der Vorlage beibehalten, um Ihre Konfigurationsinformationen zu schützen. Abhängig von der ausgewählten Option werden Ihnen die Gebühren basierend auf der Menge der im Amazon S3-Bucket gespeicherten Daten und der Anzahl der Git-Anforderungen (nicht für Amazon S3-Ressourcen anwendbar) berechnet. Einzelheiten finden Sie unter Amazon S3 und AWS CodeCommit-Preise.

Komponentenservices

Die folgenden AWS Services sind Komponenten von Customizations for AWS Control Tower (CfCT).

AWS CodeCommit

Basierend auf Ihren Eingaben für die AWS CloudFormation Vorlage kann CfCT ein -AWS CodeCommitRepository mit derselben Beispielkonfiguration erstellen, die im Abschnitt Amazon Simple Storage Service erläutert wird.

Um das CfCT AWS CodeCommit -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 für AWS CodeCommit.

AWS CodePipeline

AWS CodePipeline validiert, testet und implementiert Änderungen basierend auf Aktualisierungen des Konfigurationspakets, die Sie entweder im standardmäßigen Amazon S3-Bucket oder im AWS CodeCommit Repository vornehmen. Weitere Informationen zum Ändern der Kontrolle der Konfigurationsquelle in AWS CodeCommitfinden Sie unter Verwenden von Amazon S3 als Konfigurationsquelle. Die Pipeline umfasst Phasen zur Validierung und Verwaltung der Konfigurationsdateien und -vorlagen, Kernkonten, AWS Organizations Service-Kontrollrichtlinien und AWS CloudFormation StackSets. 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 sensible Parameter im AWS Systems Manager Parameter Store zu verschlüsseln. Standardmäßig sind nur von CfCT bereitgestellte Rollen berechtigt, Verschlüsselungs- oder Entschlüsselungsvorgänge mit diesem Schlüssel durchzuführen. Für den Zugriff auf die Konfigurationsdatei, FIFO-Warteschlange oder Parameter Store-`SecureString`Werte müssen Administratoren zur `CustomControlTowerKMSKey` Richtlinie hinzugefügt werden. Die automatische Schlüsseldrehung 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 Lebenszyklusereignisses von AWS Control Tower aufzurufen.

Amazon Simple Notification Service

CfCT kann während des Workflows Benachrichtigungen veröffentlichen, z. B. die Pipeline-Genehmigung in Amazon Simple Notification Service (Amazon SNS)-Themen. Amazon SNS wird nur gestartet, wenn Sie Pipeline-Genehmigungsbenachrichtigungen erhalten möchten.

Amazon Simple Storage Service

Wenn Sie CfCT bereitstellen, erstellt CfCT einen Amazon Simple Storage Service (Amazon S3)-Bucket mit einem eindeutigen Namen:

Beispiel: Amazon S3-Bucket-Name

`custom-control-tower-configuration-accountID-region`

Der Bucket enthält eine Beispielkonfigurationsdatei namens `_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 Landing Zone von AWS Control Tower. Das Beispielmanifest identifiziert die erforderlichen Konfigurationen für Stack-Sets und Service-Kontrollrichtlinien (SCPs), die Sie bei der Implementierung Ihrer Anpassungen benötigen.

Sie können dieses Beispielkonfigurationspaket als Modell verwenden, um Ihr benutzerdefiniertes Paket zu entwickeln und hochzuladen, wodurch die CfCT-Konfigurationspipeline automatisch ausgelöst wird.

Informationen zum Anpassen der Konfigurationsdatei finden Sie unter Leitfaden zur cFcT-Anpassung.

Amazon Simple Queue Service

CfCT verwendet eine Amazon Simple Queue Service (Amazon SQS) FIFO-Warteschlange, um Lebenszyklusereignisse von Amazon zu erfassen EventBridge. Es löst eine - AWS Lambda Funktion aus, die aufruft, AWS CodePipeline um AWS CloudFormation StackSets oder SCPs bereitzustellen. Weitere Informationen zu SCPs finden Sie unter AWS Organizations.

AWS Step Functions

CfCT erstellt Step Functions, um Anpassungsbereitstellungen zu orchestrieren. Diese Step Functions übersetzen Konfigurationsdateien, um die Anpassungen nach Bedarf in allen Umgebungen bereitzustellen.

AWS Systems Manager Parameter Store

AWS Systems Manager Parameter Store speichert die CfCT-Konfigurationsparameter. Mit diesen Parametern können Sie zugehörige 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 anzeigen können.

Überlegungen zur Bereitstellung

Stellen Sie sicher, dass Sie Anpassungen für AWS Control Tower (CfCT) in demselben Konto und derselben Region starten, in der Ihre Landing Zone von AWS Control Tower bereitgestellt wird. Das heißt, Sie müssen sie im AWS Control Tower-Verwaltungskonto in Ihrer AWS Control Tower-Heimatregion bereitstellen. Standardmäßig erstellt CfCT das Landing Zone-Konfigurationspaket und führt es aus, indem es eine Konfigurationspipeline in diesem Konto und dieser Region einrichtet.

Vorbereiten der Bereitstellung

Sie haben einige Optionen, wenn Sie Ihre AWS 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 zum Speichern des Beispielkonfigurationspakets als `.zip` Datei namens `_custom-control-tower-configuration.zip`. Der Amazon S3-Bucket wird versionsgesteuert und Sie können das Konfigurationspaket nach Bedarf aktualisieren. Informationen zum Aktualisieren des Konfigurationspakets finden Sie unter Verwenden von Amazon S3 als Konfigurationsquelle.

> **Hinweis**
>
> Der Dateiname des Beispielkonfigurationspakets beginnt mit einem Unterstrich (_), sodass nicht automatisch initiiert AWS CodePipeline wird. Wenn Sie mit der Anpassung des Konfigurationspakets fertig sind, stellen Sie sicher, dass Sie die `custom-control-tower-configuration.zip` ohne Unterstrich (_) hochladen, um die Bereitstellung in zu starten AWS CodePipeline.

Sie können den Speicherort des Konfigurationspakets vom S3-Bucket in ein AWS CodeCommit Git-Repository ändern, indem Sie die `AWS CodeCommit` Option im AWS CloudFormation Parameter auswählen. Mit dieser Option können Sie die Versionskontrolle einfach verwalten.

> **Hinweis**
>
> 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, stellen Sie sicher, dass das Konfigurationspaket ohne Komprimierung der Dateien im Repository abgelegt ist. Informationen zum Erstellen und Speichern des Konfigurationspakets in finden Sie AWS CodeCommitunter Leitfaden 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-Bucket oder in das AWS CodeCommit Repository. Die Pipeline beginnt automatisch, wenn Sie die Konfigurationsdatei hochladen.

> **Hinweis**
>
> Wenn Sie AWS CodeCommit zum Speichern des Konfigurationspakets verwenden, ist es nicht erforderlich, das Paket zu komprimieren. Informationen zum Erstellen und Speichern des Konfigurationspakets in AWS CodeCommitfinden Sie unter Leitfaden zur cFcT-Anpassung.

Wählen Sie die Genehmigungsparameter für Ihre 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 unter Schritt 1. Starten Sie den Stack .

Wenn die manuelle Genehmigung aktiviert ist, validiert die Konfigurations-Pipeline die am AWS Control Tower-Dateimanifest und den Vorlagen vorgenommenen Anpassungen und pausiert dann den Prozess, bis die manuelle Genehmigung erteilt wird. Nach der Genehmigung führt die Bereitstellung nach Bedarf die verbleibenden Pipeline-Phasen aus, um die Funktionalität Anpassungen für AWS Control Tower (CfCT) zu implementieren.

Sie können den manuellen Genehmigungsparameter verwenden, um zu verhindern, dass die Anpassungen für die AWS Control Tower-Konfiguration ausgeführt werden, indem Sie den ersten Versuch, die Pipeline zu durchlaufen, ablehnen. Mit diesem Parameter können Sie auch Anpassungen für die AWS Control Tower-Konfigurationsänderungen manuell als endgültige Kontrolle vor der Implementierung überprüfen.

So aktualisieren Sie Anpassungen für AWS Control Tower

Wenn Sie zuvor CfCT AWS CloudFormation bereitgestellt haben, müssen Sie den Stack aktualisieren, um die neueste Version des CfCT-Frameworks zu erhalten. Weitere Informationen finden Sie unter Aktualisieren des Stacks.

Vorlage und Quellcode

Anpassungen für AWS Control Tower (CfCT) werden in Ihrem Verwaltungskonto bereitgestellt, nachdem Sie Ihre AWS CloudFormation Vorlage gestartet haben. Sie können die Vorlage von GitHub herunterladen und dann von startenAWS CloudFormation.

Die customizations-for-aws-control-tower.template stellt Folgendes bereit:

- Ein - AWS CodeBuild Projekt
- Ein - AWS CodePipeline Projekt
- Eine Amazon- EventBridge 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 GitHub Repository besuchen, um die Vorlagen und Skripts für CfCT herunterzuladen und Ihre Landing Zone-Anpassungen mit anderen zu teilen.

Automatisierte Bereitstellung

Bevor Sie die automatisierte Bereitstellung starten, lesen Sie die Überlegungen . Folgen Sie den step-by-step Anweisungen in diesem Abschnitt, um die Lösung zu konfigurieren und in Ihrem AWS Control Tower-Verwaltungskonto bereitzustellen.

Bereitstellungszeit: ungefähr 15 Minuten

Voraussetzungen

CfCT muss in Ihrem AWS Control Tower-Verwaltungskonto und in Ihrer AWS Control Tower-Heimatregion bereitgestellt werden. Wenn Sie keine Landing Zone eingerichtet haben, finden Sie weitere Informationen unter Erste 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 AWS CloudFormation Vorlage in Ihrem Verwaltungskonto.
- Überprüfen Sie die Vorlagenparameter und passen Sie sie bei Bedarf an.

Schritt 2. Erstellen eines benutzerdefinierten Pakets

- 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 AWS 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 während der Ausführung von CfCT verwendet werden. Weitere Details finden Sie unter 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 dem Sie Ihre Landing Zone von AWS Control Tower bereitgestellt haben, die Ihre Heimatregion ist.

3. Überprüfen Sie auf der Seite Stack erstellen, ob die richtige Vorlagen-URL im Textfeld URL 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.

Pipeline-Konfiguration		
Parameter	Standard	Beschreibung
Pipeline-Genehmigungsphase	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

Pipeline-Konfiguration		
Parameter	Standard	Beschreibung
		“Leitfaden zur cFcT-Anpassung”.
E-Mail-Adresse der Pipeline-Genehmigung	<Optionale Eingabe>	Die E-Mail-Adresse für Genehmigungsbenachrichtigungen. Um diesen Parameter zu verwenden, müssen Sie den Parameter Pipeline-Genehmigungsstufe auf setzen`Yes`.
AWS CodePipeline-Quelle	`Amazon S3`	Die Quelle für AWS CodePipeline , mit der Sie auswählen können, wo die CfCT-Anpassungen gespeichert und konfiguriert werden sollen.
AWS CodeCommit -Einrichtung		
Parameter	Standard	Beschreibung
CodeCommitBestehendes Repository?	`No`	Wählen Sie aus, ob ein vorhandenes CodeCommit Git-Repository verwendet werden soll. Wenn Sie wählen`Yes`, müssen Sie den CodePipeline Quellparameter auf setzen`AWS CodeCommit` .

AWS CodeCommit -Einrichtung		
Parameter	Standard	Beschreibung
CodeCommit Repository-Name	`custom-control-tower-configuration`	Der Name des Git-Repositorys. Um diesen Parameter zu verwenden, müssen Sie den AWS CodePipeline-Quellparameter auf setzen`AWS CodeCommit` . Dieser Name wird verwendet, um ein neues Git-Repository zu erstellen, und muss eindeutig sein. Wenn Sie den Namen eines vorhandenen Git-Repositorys angeben, müssen Sie den Parameter Vorhandenes CodeCommit Repository? auf Ja setzen und den genauen Namen dieses Repositorys eingeben.
CodeCommit Branch-Name	`main`	Der Git-Zweig, in dem das Anpassungspaket gespeichert ist. Git-Repositorys können viele Verzweigungen haben. Dies ist der Standardname, der dem Zweig im Git-Repository gegeben wird. Um diesen Parameter zu verwenden, müssen Sie den CodePipeline Quellparameter auf setzen`AWS CodeCommit` .

AWS- CloudFormation StackSets Konfiguration		
Parameter	Standard	Beschreibung
Regions-Gleichzeitigkeitstyp	`PARALLEL`	Wählen Sie den Paralleli tätstyp von StackSets Bereitstellungsvorgängen in -Regionen aus. Diese Einstellung gilt für Erstellun gs-, Aktualisierungs- und Lösch-Workflows. Ein anderer zulässiger Wert ist `SEQUENTIAL` .
Maximaler gleichzeitiger Prozentsatz	`100`	Der maximale Prozentsa tz der Konten, auf denen dieser Vorgang gleichzeitig ausgeführt werden kann. Der maximal zulässige Wert ist 100. Weitere Informationen finden Sie unter Stack-Set-Operationsoptionen.
Prozentsatz der Fehlertol eranz	`10`	Der Prozentsatz der Konten pro Region, bei denen dieser Stack-Vorgang fehlschla gen kann, bevor AWS den Vorgang in dieser Region CloudFormation beendet. Der minimal zulässige Wert ist 0 und der maximal zulässige Wert ist 100. Weitere Informationen finden Sie unter Stack-Set-Operatio nsoptionen.

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 - AWS CloudFormation Konsole in der Spalte Status anzeigen. Sie sollten in etwa 15 Minuten den Status CREATE_COMPLETE sehen.

Schritt 2. Erstellen eines benutzerdefinierten Pakets

Mit dem gestarteten Stack können Sie Ihrer Landing Zone und Ihren Service-Kontrollrichtlinien (SCPs) von AWS Control Tower Anpassungen hinzufügen, indem Sie das enthaltene Konfigurationspaket anpassen. Detaillierte Anweisungen zum Erstellen eines benutzerdefinierten Pakets finden Sie unter Leitfaden zur cFcT-Anpassung.

> **Hinweis**
>
> Die Pipeline wird nicht ausgeführt, ohne das benutzerdefinierte Konfigurationspaket hochzuladen.

Aktualisieren des Stacks

Wenn Sie zuvor Anpassungen für AWS Control Tower (CfCT) bereitgestellt haben, befolgen Sie das Verfahren, um den AWS CloudFormation Stack für die neueste Version des CfCT-Frameworks zu aktualisieren.

> **Important**
>
> Bevor Sie das folgende Verfahren ausführen können, müssen Sie die neueste Vorlage von GitHub in einen 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 Benutzerhandbuch für Amazon Simple Storage Service.

1. Melden Sie sich an der AWS CloudFormation -Konsole an.

2. Wählen Sie Ihre vorhandenen Anpassungen für AWS Control Tower (CfCT CloudFormation)-Stack und 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 für 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 zu Amazon S3 hochgeladen GitGub haben, und wählen Sie dann Weiter aus.
   c. Überprüfen Sie, ob die Vorlagen-URL korrekt ist. Wählen Sie dann erneut Weiter und Weiter aus.
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 für Details zu den Parametern.
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, um zu bestätigen, 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 anzeigen. Sie sollten den Status UPDATE_COMPLETE in etwa 15 Minuten sehen.

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 wird keine Aktion ausgeführt, um das zugehörige Stack-Set zu löschen, wenn eine Ressource aus der CfCT-Manifestdatei entfernt wird.

Wenn Sie den Wert von `true` in der Manifestdatei `enable_stack_set_deletion` in ändern, löscht CfCT das Stack-Set und alle seine Ressourcen, wenn Sie eine zugeordnete Ressource aus der Manifestdatei entfernen.

Diese Funktion wird in v2 der Manifestdatei unterstützt.

> **Important**
>
> Wenn Sie den Wert von anfänglich `enable_stack_set_deletion` auf festlegen`true`, werden beim nächsten Aufrufen von CfCT alle Ressourcen, die mit dem Präfix beginnen`CustomControlTower-`, die das zugehörige Schlüssel-Tag haben `Key:AWS_Solutions, Value: CustomControlTowerStackSet`und die nicht in der Manifestdatei deklariert sind, zum Löschen bereitgestellt.

Im Folgenden finden Sie ein Beispiel dafür, wie Sie diesen Parameter in einer `manifest.yaml` Datei festlegen:

```
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
```

Einrichten von Amazon S3 als Konfigurationsquelle

Wenn Sie Anpassungen für AWS Control Tower einrichten, speichert es eine anfängliche Konfigurationsdatei namens `_custom-control-tower-configuration.zip` Datei in einem Amazon Simple Storage Service (Amazon S3)-Bucket namens `custom-control-tower-configuration-`*`account-ID`*`-`*`region`*.

> **Hinweis**
>
> Wenn Sie diese Datei herunterladen und ändern möchten, denken Sie daran, die Änderungen zu komprimieren, als neue Datei mit dem Namen zu speichern `custom-control-tower-configuration.zip`und sie dann wieder in denselben Amazon S3-Bucket hochzuladen.
> Der Amazon S3-Bucket ist die Standardquelle der Pipeline. Wenn Standardeinstellungen vorhanden sind, wird das Hochladen einer Konfigurations-ZIP-Datei ohne Unterstrichpräfix 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) geschützt und die Verwendung des KMS-Schlüssels wird verweigert. Für den Zugriff auf die ZIP-Datei müssen Sie die KMS-Schlüsselrichtlinie aktualisieren, um die Rolle(n) anzugeben, denen Zugriff gewährt werden soll. Die Rolle kann eine Administratorrolle, ein Benutzer oder beides sein. Gehen Sie wie folgt vor:

1. Navigieren Sie zur AWS Key Management Service -Konsole.
2. Wählen Sie unter Kundenverwaltete Schlüssel die Option CustomControlTowerKMSKey aus.
3. Wählen Sie die Registerkarte Schlüsselrichtlinie aus. Wählen Sie dann Bearbeiten aus.
4. Suchen Sie auf der Seite Schlüsselrichtlinie bearbeiten im Abschnitt Verwendung des Schlüssels zulassen im Code und fügen Sie eine der folgenden Berechtigungen hinzu:
   - So fügen Sie eine -Administratorrolle hinzu:

```
arn:aws:iam::<account-ID>:role/<administrator-role>
```

- So fügen Sie einen Benutzer hinzu:

```
arn:aws:iam::<account-ID>:user/<username>
```

5. Wählen Sie Save Changes (Änderungen speichern).
6. Navigieren Sie zur Amazon S3-Konsole , suchen Sie den S3-Bucket mit der Konfigurations-ZIP-Datei und wählen Sie Herunterladen aus.
7. Nehmen Sie die erforderlichen Konfigurationsänderungen an der Manifestdatei und den Vorlagendateien vor. Informationen zum Anpassen des Manifests und der Vorlagendateien finden Sie unter the section called “Leitfaden zur cFcT-Anpassung”.
8. Laden Sie Ihre Änderungen hoch:
   a. Komprimieren Sie die geänderten Konfigurationsdateien und benennen Sie die Datei: `custom-control-tower-configuration.zip`.
   b. Laden Sie die Datei mit SSE mit dem AWS KMS Master-Schlüssel zu Amazon S3 hoch: `CustomControlTowerKMSKey`.

Sammlung von Betriebsmetriken

Anpassungen für AWS Control Tower (CfCT) enthält eine Option zum Senden anonymer Betriebsmetriken an AWS. AWS verwendet diese Daten, um zu verstehen, wie Kunden CfCT sowie andere zugehörige -Services und -Produkte verwenden. Wenn die Datenerfassung aktiviert ist, werden die folgenden Informationen an gesendet AWS:

- Lösungs-ID: Die AWS Lösungs-ID
- Eindeutige ID (UUID): Zufällig generierte, eindeutige Kennung für jede Bereitstellung
- Zeitstempel: Zeitstempel der Datenerfassung
- Anzahl der Ausführung von Zustandsautomaten: Zählt inkrementell, wie oft dieser Zustandsautomat ausgeführt wird
- Manifestversion: Die in der Konfiguration verwendete Manifestversion

> **Note**
>
> AWS besitzt die gesammelten Daten. Die Datenerfassung unterliegt der AWS Datenschutzrichtlinie .

Führen Sie eine der folgenden Aufgaben aus AWS, um das Senden anonymer Betriebsmetriken an zu deaktivieren:

- Aktualisieren Sie den AWS CloudFormation Vorlagenzuordnungsabschnitt 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 Customizations for AWS Control Tower (cFCT) richtet sich an Administratoren, DevOps Fachleute, unabhängige Softwareanbieter, IT-Infrastrukturarchitekten und Systemintegratoren, die ihre AWS Control Tower Tower-Umgebungen für ihr Unternehmen und ihre Kunden anpassen und erweitern möchten. Es enthält Informationen zur Anpassung und Erweiterung der AWS Control Tower 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 Prozess detailliert 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 Manifest-Datei
- Ein begleitender Satz von Vorlagen
- Andere JSON-Dateien zur Beschreibung und Implementierung Ihrer AWS Control Tower Tower-Umgebungsanpassungen

Standardmäßig wird das `_custom-control-tower-configuration.zip` Konfigurationspaket in einen Amazon S3 S3-Bucket mit der folgenden Namenskonvention geladen:

`custom-control-tower-configuration-`*`accountID`*`-`*`region`*.

> **Note**
>
> Standardmäßig erstellt CfCT einen Amazon S3 S3-Bucket zum Speichern der Pipeline-Quelle, aber Sie können den Quellspeicherort in ein AWS CodeCommit Repository ändern. Weitere Informationen finden Sie unter Bearbeiten einer Pipeline CodePipeline im AWS CodePipeline Benutzerhandbuch.

Die Manifestdatei ist eine Textdatei, die die AWS Ressourcen beschreibt, die Sie einsetzen können, um Ihre landing zone anzupassen. CodePipeline führt die folgenden Aufgaben aus:

- extrahiert die Manifest-Datei, den dazugehörigen Satz von Vorlagen und andere JSON-Dateien
- führt Manifest- und Vorlagenvalidierungen durch
- ruft Abschnitte in der 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

> **Note**
>
> Der Dateiname des Beispielkonfigurationspakets beginnt mit einem Unterstrich (_), sodass dieser nicht automatisch ausgelöst AWS CodePipeline wird. Wenn Sie die Anpassung des Konfigurationspakets abgeschlossen haben, laden Sie die Datei `custom-control-tower-configuration.zip` ohne den Unterstrich (_) hoch, um die Bereitstellung in auszulösen. AWS CodePipeline

AWS CodePipeline Stufen

Die CfCT-Pipeline erfordert mehrere AWS CodePipeline Phasen, um Ihre AWS Control Tower Tower-Umgebung zu implementieren und zu aktualisieren.

1. Phase „Quelle“

   Die Quellphase ist die Anfangsphase. Ihr benutzerdefiniertes Konfigurationspaket leitet diese Pipeline-Phase ein. Die Quelle für AWS CodePipeline kann entweder ein Amazon S3 S3-Bucket oder ein AWS CodeCommit Repository sein, in dem das Konfigurationspaket gehostet werden kann.
2. Phase der Erstellung

   In der Erstellungsphase AWS CodeBuild muss der Inhalt des Konfigurationspakets validiert werden. Diese Prüfungen umfassen das Testen der `manifest.yaml` Dateisyntax und des Schemas sowie aller AWS CloudFormation Vorlagen, die im Paket enthalten sind oder remote gehostet werden, mithilfe von AWS CloudFormation `validate-template` und`cfn_nag`. Wenn die Manifestdatei und die AWS 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 Phase der manuellen Genehmigung 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 der Richtlinie zur Servicesteuerung

   In der Phase der Dienststeuerungsrichtlinie wird die Statusmaschine für die Dienststeuerungsrichtlinie aufgerufen, um AWS Organizations APIs aufzurufen, die Dienststeuerungsrichtlinien (SCPs) erstellen.

5. CloudFormation AWS-Ressourcenphase

   In der AWS CloudFormation Ressourcenphase wird die Stackset-Zustandsmaschine aufgerufen, um die Ressourcen bereitzustellen, die in der Liste der Konten oder Organisationseinheiten (OUs) angegeben sind, die Sie in der Manifestdatei angegeben haben. Die Zustandsmaschine erstellt die AWS CloudFormation Ressourcen in der Reihenfolge, in der sie in der Manifestdatei angegeben sind, sofern keine Ressourcenabhängigkeit angegeben ist.

Definieren Sie eine benutzerdefinierte Konfiguration

Sie definieren Ihre benutzerdefinierte AWS Control Tower Tower-Konfiguration mit der Manifestdatei, den zugehörigen Vorlagen und anderen JSON-Dateien. Sie packen diese Dateien in eine Ordnerstruktur und platzieren sie als `.zip` Datei im Amazon S3 S3-Bucket, wie im folgenden Codebeispiel gezeigt.

Ordnerstruktur mit benutzerdefinierter Konfiguration

```
- 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 eine `custom-control-tower-configuration.zip` Datei und laden Sie nur die `.zip` Datei in den dafür vorgesehenen Amazon S3 S3-Bucket hoch.

> **Note**
>
> Wenn Sie verwenden AWS CodeCommit, platzieren Sie die Dateien im Repository, ohne die Dateien zu komprimieren.

Die Manifest-Datei

Die `manifest.yaml` Datei ist eine Textdatei, die Ihre AWS Ressourcen beschreibt. Das folgende Beispiel zeigt die Struktur der Manifestdatei.

```
---
region: String
version: 2021-03-15

resources:
  #set of CloudFormation resources or SCP 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 AWS Control Tower Tower-Standardregion. Dieser Wert muss ein gültiger AWS Regionsname sein (z. B. `us-east-1`eu-west-1, oderap-southeast-1). Die AWS Control Tower Tower-Heimatregion ist die Standardeinstellung, wenn Sie benutzerdefinierte AWS Control Tower Tower-Ressourcen (wie AWS CloudFormation StackSets) erstellen, sofern keine ressourcenspezifischere Region angegeben ist.

```
region:your-home-region
```

Version — Die Versionsnummer des Manifestschemas. Die letzte unterstützte Version ist 2021-03-15.

```
version: 2021-03-15
```

> **Note**
>
> Wir empfehlen Ihnen dringend, die neueste Version zu verwenden. Informationen zum Aktualisieren der Manifesteigenschaften in der neuesten Version finden Sie unterManifeste Versionsupgrades.

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 Manifestdatei

In diesem Thema wird der Abschnitt Ressourcen der Manifestdatei beschrieben, in dem Sie die Ressourcen definieren, die für Ihre Anpassungen erforderlich sind. Dieser Abschnitt der Manifestdatei beginnt mit dem Schlüsselwort resources und setzt sich bis zum Ende der Datei fort.

Der Abschnitt Resources der Manifestdatei spezifiziert die AWS CloudFormation StackSets oder AWS Organizations SCPs, die CfcT automatisch über die Code-Pipeline bereitstellt. Sie können Organisationseinheiten, Konten und Regionen für die Bereitstellung von Stack-Instances auflisten.

Stack-Instances werden auf Kontoebene statt auf OU-Ebene bereitgestellt. SCPs werden auf OU-Ebene bereitgestellt. Weitere Informationen finden Sie unter Erstellen eigener Anpassungen.

In der folgenden Beispielvorlage werden die möglichen Einträge beschrieben, die für den Ressourcenbereich 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
    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 Schlüsselwörter, die im vorherigen Codebeispiel gezeigt wurden.

Name — Der Name, der mit dem verknüpft ist AWS 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 Unterstrich (_). Jedes andere Zeichen wird automatisch durch einen Unterstrich (_) ersetzt.

Beschreibung — Die Beschreibung der Ressource.

- Typ: Zeichenfolge
- Required: No

resource_file — Diese Datei kann als relativer Speicherort zur Manifestdatei angegeben werden, als Amazon S3 S3-URI oder URL, die auf eine AWS CloudFormation Vorlage oder AWS Organizations Service Control-Richtlinie in JSON zur Erstellung von AWS CloudFormation Ressourcen oder SCPs verweist.

- Typ: Zeichenfolge
- Erforderlich: Ja

1. Das folgende Beispiel zeigt den`resource_file`, der als relativer Speicherort zur Ressourcendatei im Konfigurationspaket angegeben wird.

```
resources:
  - name: SecurityRoles
    resource_file: templates/custom-security.template
```

2. Das folgende Beispiel zeigt die als Amazon S3 S3-URI angegebene Ressourcendatei

```
resources:
  - name: SecurityRoles
    resource_file: s3://bucket-name/[key-name]
```

3. Das folgende Beispiel zeigt die Ressourcendatei, die als Amazon S3 S3-HTTPS-URL angegeben ist.

```
resources:
  - name: SecurityRoles
    resource_file: https://bucket-name.s3.Region.amazonaws.com/key-name
```

> **Note**
>
> Wenn Sie eine Amazon S3 S3-URL angeben, stellen Sie sicher, dass die Bucket-Richtlinie Lesezugriff für das AWS Control Tower Tower-Verwaltungskonto zulässt, von dem aus Sie CfCT bereitstellen. Wenn Sie eine Amazon S3 S3-HTTPS-URL angeben, stellen Sie sicher, dass der Pfad die Punktnotation verwendet. z. B. `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 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 einsetzt. Weitere Beispiele finden Sie unter Beispiele für Bucket-Richtlinien im Amazon Simple Storage Service-Benutzerhandbuch.

parameters — Gibt den Namen und den Wert für AWS CloudFormation Parameter an.

- Typ: MapList
- Required: No

Der Parameterbereich enthält Paare von Schlüssel-/Wertparametern. Die folgende Pseudovorlage beschreibt den Abschnitt mit den Parametern.

```
parameters:
  - parameter_key: [String]
    parameter_value: [String]
```

- parameter_key — Der dem Parameter zugeordnete Schlüssel.
  - Typ: Zeichenfolge
  - Erforderlich: Ja (unter der Eigenschaft parameters)
  - Gültige Werte: a-z, A-Z und 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 durch oder mit der `scp` Option AWS CloudFormation StackSets, wenn Sie SCPs bereitstellen.

- Typ: Zeichenfolge
- Gültige Werte: `stack_set` | `scp`
- Erforderlich: Ja

deployment_targets — Liste der Konten oder Organisationseinheiten (OUs), in denen CfCT die AWS CloudFormation Ressourcen bereitstellen wird, die als Konten oder Organisationseinheiten angegeben sind.

> **Note**
>
> Wenn Sie ein SCP bereitstellen möchten, muss es sich bei dem Ziel um eine Organisationseinheit und nicht um ein Konto handeln.

- Typ: Zeichenkettenliste `account name` oder `account number` um anzugeben, dass diese Ressource in der angegebenen Kontoliste bereitgestellt wird, oder `0U names` um anzugeben, dass diese Ressource in der angegebenen OU-Liste bereitgestellt wird.
- Erforderlich: Mindestens eines der Konten oder Organizational_Units
  - Konten:

    Typ: Zeichenkettenliste `account name` oder `account number` um anzugeben, dass diese Ressource in der angegebenen Kontoliste bereitgestellt wird.
  - organisational_units:

    Typ: Zeichenkettenliste`0U 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 nicht die Bereitstellung von Stack-Instances im Verwaltungskonto der Organisation.

export_outputs — Liste von Name/Wert-Paaren, die SSM-Parameterschlüssel bezeichnen. Mit diesen SSM-Parameterschlüsseln können Sie Vorlagenausgaben im SSM-Parameterspeicher speichern. Die Ausgabe ist für die Referenzierung durch andere Ressourcen vorgesehen, die zuvor in der Manifestdatei definiert wurden.

```
export_outputs: # List of SSM parameters
  - name: [String]
    value: [String]
```

- Typ: Liste von Schlüsselpaaren aus Name und Wert. Der Name enthält die `name` Zeichenfolge eines SSM-Parameterspeicherschlüssels, und der Wert enthält die `value` Zeichenfolge des Parameters.
- Gültige Werte: Eine beliebige Zeichenfolge oder `$[output_`*`CfnOutput-Logical-ID`*`]` Variable, wobei *`CfnOutput-Logical-ID`* der Vorlagenausgabevariablen entspricht. Weitere Informationen zum Abschnitt Ausgaben in einer AWS CloudFormation Vorlage finden Sie im Benutzerhandbuch unter Ausgaben.AWS CloudFormation
- Required: No

Der folgende Codeausschnitt speichert beispielsweise die `VPCID` Ausgabevariable der Vorlage in dem benannten SSM-Parameterschlüssel. `/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 sein. `production`

Regionen — Liste der Regionen, in denen CfCT die AWS CloudFormation Stack-Instances bereitstellen wird.

- Typ: Eine beliebige Liste mit Namen AWS kommerzieller Regionen, um anzugeben, dass diese Ressource in der angegebenen Regionsliste bereitgestellt wird. Wenn dieses Schlüsselwort nicht in der Manifestdatei vorhanden ist, werden die Ressourcen nur in der Heimatregion bereitgestellt.
- Required: No

Stamm-OU

CFCT unterstützt Root als Wert für eine Organisationseinheit (OU) `organizational_units` in der Manifest V2-Version (2021-03-15).

- Wenn Sie die Bereitstellungsmethode wählen und Root unter hinzufügen`organizational_units`, wendet AWS Control Tower die Richtlinien auf alle Organisationseinheiten unter dem Root an. `scp` Wenn Sie die Bereitstellungsmethode von `stack_set` wählen und Root unter hinzufügen`organizational_units`, stellt CfCT die Stack-Sets in allen Konten unter dem Root bereit, die in AWS Control Tower registriert sind, mit Ausnahme des Verwaltungskontos.
- Gemäß den Best Practices von AWS Control Tower ist das Verwaltungskonto nur für die Verwaltung von Mitgliedskonten und für Abrechnungszwecke vorgesehen. Führen Sie keine Produktionsworkloads im AWS Control Tower Tower-Managementkonto aus.

  Gemäß den Richtlinien für bewährte Methoden wird bei der Bereitstellung von AWS Control Tower das Verwaltungskonto unter die Root-OU gestellt, sodass es vollen Zugriff hat und keine zusätzlichen Ressourcen ausführt. Aus diesem Grund wird die AWSControlTowerExecutionRolle nicht für das Verwaltungskonto bereitgestellt.
- Wir empfehlen Ihnen, diese bewährten Methoden für das Verwaltungskonto zu befolgen. Wenn Sie einen bestimmten Anwendungsfall haben, bei dem Sie Stacksets im Verwaltungskonto bereitstellen müssen, geben Sie Konten als Bereitstellungsziel an 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. Andernfalls sollten Sie Konten nicht als Bereitstellungsziel angeben.

```
---
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 (2021-03-15) unterstützt. Wenn Sie Root als OU hinzufügen`organizational_units`, fügen Sie keine weiteren 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 OUs verwendet wird. Als Bereitstellungsmethode `scp` stellt AWS Control Tower die SCPs auf der letzten OU im verschachtelten OU-Pfad bereit. Als Bereitstellungsmethode `stack_set` stellt AWS Control Tower die Stack-Sets für alle Konten unter der letzten OU im verschachtelten OU-Pfad bereit.

Betrachten Sie zum Beispiel den Pfad. `OUName1:OUName2:OUName3` Die letzte Organisationseinheit im Pfad ist`OUName3`. CfCT stellt die SCPs nur auf allen Konten bereit, die sich direkt darunter `OUName3` befinden, `OUName3` und stapelt Sets für sie.

```
---
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 vorzunehmen, können Sie die `manifest.yaml` Datei ändern, indem Sie Service Control-Richtlinien (SCPs) und AWS CloudFormation Ressourcen hinzufügen oder aktualisieren. 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 Hauptbestandteile der Erstellung eigener Anpassungen erläutert:

- wie Sie Ihr eigenes Konfigurationspaket für Richtlinien zur Servicesteuerung einrichten
- wie Sie Ihr eigenes Konfigurationspaket für AWS CloudFormation Stack-Sets einrichten

Richten Sie ein Konfigurationspaket für Richtlinien zur Servicesteuerung ein

In diesem Abschnitt wird erklärt, wie Sie ein Konfigurationspaket für Service Control Policies (SCPs) erstellen. Die beiden Hauptteile dieses Prozesses sind (1) die Vorbereitung der 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 `resource_file` und `deployment_targets` -Details hinzu.

Das folgende Snippet zeigt die Standard-Manifestdatei.

```
---
region: us-east-1
version: 2021-03-15

resources: []
```

Der Wert für `region` wird bei der Bereitstellung automatisch hinzugefügt. Er muss mit der Region übereinstimmen, in der Sie CfCT bereitgestellt haben. Diese Region muss mit der AWS Control Tower Tower-Region identisch sein.

Um dem `example-configuration` Ordner im Zip-Paket, das im Amazon S3-Bucket gespeichert ist, ein benutzerdefiniertes SCP 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
    #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
    #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 S3-URL für die Ressourcendatei verwenden und Parameter mit Schlüssel/Wert-Paaren verwenden.

Sie müssen eine SCP-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 JSON-Richtliniendatei enthält die SCPs, die für Organisationseinheiten 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`

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"GuardPutAccountPublicAccessBlock",
         "Effect":"Deny",
         "Action":"s3:PutAccountPublicAccessBlock",
         "Resource":"arn:aws:s3:::*"
      }
   ]
}
```

Richten Sie ein Konfigurationspaket ein für AWS CloudFormation StackSets

In diesem Abschnitt wird erklärt, wie Sie ein Konfigurationspaket für AWS CloudFormation StackSets einrichten. Die beiden Hauptteile dieses Prozesses sind: (1) Vorbereitung der Manifestdatei und (2) Aktualisierung der Ordnerstruktur.

Schritt 1: Bearbeiten Sie die bestehende Manifestdatei

Fügen Sie die neuen AWS CloudFormation StackSets Informationen zur Manifestdatei hinzu, die Sie zuvor bearbeitet haben.

Nur zur besseren Übersicht: Der folgende Ausschnitt enthält dieselbe benutzerdefinierte Manifestdatei, die bereits gezeigt wurde, um ein Konfigurationspaket für SCPs einzurichten. Jetzt können Sie diese Datei weiter bearbeiten, um die Details zu Ihren Ressourcen aufzunehmen.

```
---
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
    #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 entsprechend 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 AWS 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
    #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 AWS CloudFormation Vorlagendateien und SCP-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 Beispielmanifestdatei.

```
- manifest.yaml
- policies/
   - block-s3-public.json
- templates/
   - transit-gateway.template
```

Der 'alfred'-Helfer und die AWS CloudFormation Parameterdateien

CfCT bietet Ihnen einen Mechanismus, der als Alfred-Helper bekannt ist, um den Wert für einen SSM-Parameterspeicher-Schlüssel abzurufen, der in der AWS CloudFormation Vorlage definiert ist. Mit dem Alfred-Helper können Sie Werte verwenden, die im SSM-Parameterspeicher gespeichert sind, ohne die Vorlage zu aktualisieren. AWS CloudFormation Weitere Informationen finden Sie unter Was ist eine AWS CloudFormation Vorlage? im AWS CloudFormation Benutzerhandbuch.

> **Important**
>
> Der Alfred Helper hat zwei Einschränkungen. Parameter sind nur in der Heimatregion des AWS Control Tower 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

Nehmen wir an, Sie haben zwei AWS CloudFormation Stack-Sets. Stack-Set 1 hat eine Stack-Instance und wird auf einem Konto in einer Region bereitgestellt. Es erstellt eine Amazon-VPC und Subnetze in einer Availability Zone, und die `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 das `VPC ID` und mithilfe von in Stack-Set 1 gespeichert werden. `AWS:::SSM::Parameter` Weitere Informationen finden Sie unter `AWS:::SSM::Parameter` im AWS CloudFormation -Benutzerhandbuch.

AWS CloudFormation Stapelsatz 1:

Im folgenden Snippet 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
```

AWS CloudFormation Stapelsatz 2:

Das Snippet zeigt die Parameter, die in der AWS 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]
```

AWS 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 AWS 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, und es kann hilfreich sein, um Fehler beim Erstellen Ihrer eigenen `manifest.yaml` Datei zu reduzieren.

Manifeste Versionsupgrades

Informationen zur neuesten Version von Customizations for AWS Control Tower (cFCT) finden Sie in der Datei CHANGELOG.md im Repository. GitHub

Warning

In Version 2.2.0 von Customizations for AWS Control Tower (cFCT) wurde ein Manifestschema (Version 2021-03-15) eingeführt, das an die entsprechenden Service-APIs angepasst werden soll. AWS Das Manifestschema ermöglicht es einer einzigen manifest.yaml-Datei, unterstützte Ressourcen (AWS CloudFormation Vorlagen und SCPs) über entkoppelte Workflows zu verwalten. DevOps
Es wird dringend empfohlen, das 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. Version 2020-01-01 befindet sich jedoch am Ende des Support. Wir stellen keine Updates mehr bereit und fügen keine Verbesserungen zu Version 2020-01-01 mehr hinzu. Die Funktionen Root-OU und verschachtelte Organisationseinheiten werden in Version 2020-01-01 nicht unterstützt.

Veraltete Eigenschaften in der 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 Schritte zur Aktualisierung

Wenn Sie auf die Manifestschemaversion 2021-03-15 aktualisieren, müssen Sie die folgenden Änderungen vornehmen, um Ihre Dateien zu aktualisieren. In den nächsten Abschnitten werden die obligatorischen und empfohlenen Änderungen für den Übergang beschrieben.

Richtlinien von Organizations

1. Verschieben Sie die SCPs unter organization_policies unter neue Immobilienressourcen.
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 Konten wird für Unternehmensrichtlinien nicht unterstützt.
4. Fügen Sie eine neue Eigenschaft deploy_method mit dem Wert scp hinzu.

AWS 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 Kontoliste sollte unter Konten mit Untereigenschaften definiert werden.
5. Ändern Sie die Eigenschaft ssm_parameters in die neue Eigenschaft export_outputs.

Sehr empfehlenswerte Upgrade-Schritte

AWS CloudFormation Parameter

1. Ändern Sie die Eigenschaft parameter_file in neue Eigenschaftsparameter.
2. Entfernen Sie den Dateipfad aus dem 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 Parameter-Eigenschaft. Dies würde Ihnen helfen, sie in der Manifestdatei zu verwalten.

> **Note**
>
> Die Eigenschaft parameter_file wird in der 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 zur Konfiguration Ihrer VPC verwenden. Weitere Informationen zur Arbeit mit VPCs und AWS Control Tower finden Sie unter Aufbau einer skalierbaren und sicheren AWS Multi-VPC-Netzwerkinfrastruktur.

Verwandte Themen

- Informationen zur Funktionsweise von AWS Control Tower bei der Registrierung von Konten mit vorhandenen VPCs finden Sie unter. Registrierung vorhandener 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 zur Konfiguration von AWS Control Tower Tower-Konten ohne VPC finden Sie unter. Exemplarische Vorgehensweise: Konfiguration von AWS Control Tower ohne VPC
- Informationen zum Ändern der Kontoeinstellungen für VPCs finden Sie in der Account Factory 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 den zugehörigen Informationen in diesem Benutzerhandbuch.

VPCs und AWS Regionen in 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 identisch mit einer VPC, die AWS Control Tower für ein bereitgestelltes Konto erstellt, aber die AWS Standard-VPC in einer nicht verwalteten Region kann für IAM-Benutzer zugänglich sein.

Administratoren können die Region Deny Control aktivieren, sodass Ihre Endbenutzer nicht berechtigt sind, eine Verbindung zu einer VPC in einer Region herzustellen, die von AWS Control Tower unterstützt wird, aber außerhalb Ihrer kontrollierten Regionen. Um die Regionsverweigerungssteuerung zu konfigurieren, gehen Sie zur Seite mit den Einstellungen für die Landingzone und wählen Sie Einstellungen ändern aus.

Die Option „Region Deny“ blockiert API-Aufrufe an die meisten Dienste, die nicht verwaltet werden AWS-Regionen. Weitere Informationen finden Sie unter Zugriff verweigern auf AWS Grundlage der angeforderten AWS-Region Daten. .

> **Note**
>
> Die Regionsverweigerungssteuerung verhindert möglicherweise nicht, dass IAM-Benutzer eine Verbindung zu einer AWS Standard-VPC in einer Region herstellen, in der AWS Control Tower nicht unterstützt wird.

Optional können Sie die AWS Standard-VPCs in nicht verwalteten 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 entspricht nicht der AWS Standard-VPC.
- Wenn AWS Control Tower ein neues Konto in einer unterstützten AWS Region einrichtet, löscht AWS Control Tower automatisch die AWS Standard-VPC und richtet eine neue, von AWS Control Tower konfigurierte VPC ein.
- 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 in Regionen mit Ausnahme der USA West (Nordkalifornien) jede AWS Control Tower VPC 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-zu-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.

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 die Protokollierung und die Sicherheitsüberprüfung 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. Über uns AWS-Konten in 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 das StackSet- AWSControlTowerExecutionRole, um die Rolle in allen Konten in dieser Organisationseinheit zu erstellen.

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 registrieren Sie sie.

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, Vertrauensbeziehungen

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.

Um zu verhindern, dass ein Angreifer 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. Aus Sicherheitsgründen empfehlen wir dringend, die `aws:SourceArn` Bedingung hinzuzufügen, 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.

```
{
  "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, der als bezeichnet wird`controltower.amazonaws.com`.

Das nächste Beispiel zeigt die `aws:SourceArn` Bedingungen `aws:SourceAccount` und Bedingungen, die für die Vertrauensrichtlinie für Rollen gelten.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "controltower.amazonaws.com"
        ]
```

```
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "012345678901"
        },
        "StringLike": {
          "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 Vermeiden Sie dienstübergreifendes Identitätsmissbrauchs.

Allgemeine Informationen zu Berechtigungsrichtlinien in AWS Control Tower finden Sie unterZugriff auf Ressourcen verwalten.

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`.

Hier ist die IAM-Richtlinie (JSON-Artefakt), die der Rolle zugeordnet ist:

```
{
    "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 Richtlinie`AWSControlTowerServiceRolePolicy`, die von der `AWSControlTowerAdmin` Rolle bei der Erstellung des AWS Config Aggregators verwendet wird, die folgenden Berechtigungen hinzugefügt:

```
{
  "Version": "2012-10-17",
    "Statement": [
      {
        "Effect": "Allow",
        "Action": [
          "config:PutConfigurationAggregator",
          "config:DeleteConfigurationAggregator",
          "iam:PassRole"
          ],
        "Resource": [
          "arn:aws:iam:::role/service-role/
AWSControlTowerConfigAggregatorRoleForOrganizations",
          "arn:aws:config:::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.

Das AWS Control Tower Tower-Stack-Set `StackSet-AWSControlTowerBP-BASELINE-ROLES` erstellt diese ausschließlich programmgesteuerten, kontenübergreifenden Rollen im Auditkonto:

- aws-controltower- AdministratorExecutionRole
- aws-Kontrollturm- AuditAdministratorRole
- aws-Kontrollturm- ReadOnlyExecutionRole
- 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.

```
{
  "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.

```
{
  "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-AuditAdministratorRole`

```
{
  "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:GetPeregrineStatus",
                "sso:GetApplicationInstance",
                "sso:ListDirectoryAssociations",
                "sso:ListPermissionSets",
                "sso:GetPermissionSet",
                "sso:ProvisionApplicationInstanceForAWSAccount",
                "sso:ProvisionApplicationProfileForAWSAccountInstance",
                "sso:ProvisionSAMLProvider",
                "sso:ListProfileAssociations",
                "sso-directory:ListMembersInGroup",
                "sso-directory:AddMemberToGroup",
                "sso-directory:SearchGroups",
                "sso-directory:SearchGroupsWithGroupName",
                "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": "*"
        }
    ]
}
```

Die Berechtigungen `sso:GetPeregrineStatus` `sso:ProvisionApplicationInstanceForAWSAccountsso:ProvisionApplicationProfileForA` und `sso:ProvisionSAMLProvide` werden von AWS Control Tower Account Factory für die Interaktion mit dem AWS IAM Identity Center benötigt.

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 Tower-Ressourcen.
- Informationen zu Ressourcen, die AWS Control Tower in den gemeinsamen Konten erstellt, finden Sie unterÜber die gemeinsamen Konten.
- 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.

So arbeiten AWS Regionen mit AWS Control Tower

Derzeit wird AWS Control Tower 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)
- Europe (Paris)
- Südamerika (São Paulo)
- USA West (Nordkalifornien)
- Asien-Pazifik (Hongkong)
- Asien-Pazifik (Jakarta)
- Asien-Pazifik (Osaka)
- Europa (Milan)
- Afrika (Kapstadt)
- Naher Osten (Bahrain)
- Israel (Tel Aviv)
- Naher Osten (VAE)
- Europa (Spain)
- Asien-Pazifik (Hyderabad)
- Europa (Zürich)

- Asien-Pazifik (Melbourne)
- Kanada West (Calgary)

Über Ihre Heimatregion

Wenn Sie eine landing zone erstellen, wird die Region, die Sie für den Zugriff auf die AWS Management-Konsole 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.

Steuerelemente und Regionen

Derzeit funktionieren alle präventiven Kontrollen weltweit. Detective und proaktive Kontrollen funktionieren jedoch nur in Regionen, in denen AWS Control Tower unterstützt wird. Weitere Informationen zum Verhalten von Kontrollen bei der Aktivierung von AWS Control Tower in einer neuen Region finden Sie unterKonfigurieren Sie Ihre AWS Control Tower Tower-Regionen.

Konfigurieren Sie Ihre AWS Control Tower Tower-Regionen

In diesem Abschnitt wird das Verhalten beschrieben, das Sie erwarten können, wenn Sie Ihre AWS Control Tower Tower-Landezone auf eine neue AWS Region ausdehnen oder eine Region aus Ihrer Landezonenkonfiguration entfernen. Im Allgemeinen wird diese Aktion über die Aktualisierungsfunktion der AWS Control Tower Tower-Konsole ausgeführt.

> **Note**
>
> Wir empfehlen Ihnen, Ihre AWS Control Tower Tower-Landezone nicht auf AWS Regionen auszudehnen, in denen Ihre Workloads nicht ausgeführt werden müssen. Wenn Sie sich von einer Region abmelden, werden Sie nicht daran gehindert, Ressourcen in dieser Region bereitzustellen, aber diese Ressourcen bleiben außerhalb der AWS Control Tower Tower-Governance.

Während der Konfiguration einer neuen Region aktualisiert AWS Control Tower die landing zone, was bedeutet, dass Ihre landing zone als Baseline festgelegt wird —

- in allen neu ausgewählten Regionen aktiv tätig zu sein und

- die Verwaltung der Ressourcen in den abgewählten Regionen einzustellen.

Einzelne Konten innerhalb Ihrer Organisationseinheiten (OUs), die von AWS Control Tower verwaltet werden, werden im Rahmen dieses landing zone Zone-Aktualisierungsprozesses nicht aktualisiert. Daher müssen Sie Ihre Konten aktualisieren, indem Sie Ihre Organisationseinheiten erneut registrieren.

Beachten Sie bei der Konfiguration Ihrer AWS Control Tower 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 AWS Control Tower Tower-Governance.

Wenn Sie Ihre landing zone für neue Regionen konfigurieren, hält sich AWS Control Tower Detective Controls an die folgenden Regeln:

- Was vorhanden ist, bleibt gleich. Das Verhalten der Leitlinien, sowohl hinsichtlich der aufdeckenden als auch der präventiven, bleibt bei bestehenden Konten, in bestehenden OUs und in bestehenden Regionen unverändert.
- Sie können neue Detective-Kontrollen nicht auf bestehende Organisationseinheiten anwenden, die Konten enthalten, die nicht aktualisiert wurden. Wenn Sie Ihre AWS Control Tower Tower-Landezone für eine neue Region konfiguriert haben (indem Sie Ihre landing zone aktualisiert haben), müssen Sie die vorhandenen Konten in Ihren vorhandenen Organisationseinheiten aktualisieren, bevor Sie neue Detective Controls für diese OUs und Konten aktivieren können.
- Ihre vorhandenen Detective Controls funktionieren in den neu konfigurierten Regionen, sobald Sie die Konten aktualisieren. Wenn Sie Ihre AWS Control Tower Tower-Landing landing zone aktualisieren, um neue Regionen zu konfigurieren, und dann ein Konto aktualisieren, funktionieren die Detective Controls, die bereits auf der Organisationseinheit aktiviert sind, für dieses Konto in den neu konfigurierten Regionen.

AWS Control Tower Tower-Regionen konfigurieren

1. Melden Sie sich bei der AWS Control Tower Tower-Konsole an unter 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 Bereich Details oben rechts die Schaltfläche Einstellungen ändern aus. Sie werden zum Workflow „landing zone aktualisieren“ weitergeleitet, da für die Verwaltung neuer Regionen oder das Entfernen von Regionen aus der Verwaltung ein Update auf die neueste Landingzone-Version erforderlich ist.
4. Suchen Sie unter Zusätzliche AWS Regionen für die Verwaltung nach den Regionen, die Sie verwalten (oder beenden) möchten. In der Spalte Bundesland wird angezeigt, welche Regionen Sie derzeit regieren und welche nicht.
5. Aktivieren Sie das Kontrollkästchen für jede weitere Region, die verwaltet werden soll. Deaktivieren Sie das Kontrollkästchen für jede Region, aus der Sie die Verwaltung entfernen möchten.

   > **Note**
   >
   > Wenn Sie sich dafür entscheiden, eine Region nicht zu verwalten, können Sie trotzdem Ressourcen in dieser Region bereitstellen, aber diese Ressourcen bleiben außerhalb der AWS Control Tower Tower-Governance.

6. Schließen Sie den Rest des Workflows ab und wählen Sie dann landing zone aktualisieren.
7. Wenn die Einrichtung der landing zone abgeschlossen ist, registrieren Sie die Organisationseinheiten erneut, um die Konten in Ihren neuen Regionen zu aktualisieren. Weitere Informationen finden Sie unter Wann sollten AWS Control Tower-OUs und -Konten 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 gemischte Verwaltungsstrukturen bei der Konfiguration von Regionen

Es ist wichtig, alle Konten in einer Organisationseinheit zu aktualisieren AWS-Region, nachdem Sie AWS Control Tower Governance auf eine neue erweitert und AWS Control Tower Governance aus einer Region entfernt haben.

Eine gemischte Verwaltung ist eine unerwünschte Situation, die auftreten kann, wenn die für eine Organisationseinheit geltenden Kontrollen nicht vollständig mit den Kontrollen übereinstimmen, die für jedes Konto innerhalb einer Organisationseinheit gelten. Eine gemischte Governance tritt in einer Organisationseinheit auf, wenn Konten nicht aktualisiert werden, nachdem 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 Organisationseinheit in verschiedenen Regionen unterschiedliche Kontrollen angewendet werden, und zwar im Vergleich zu anderen Konten in der Organisationseinheit oder im Vergleich zum allgemeinen Governance-Status der Landing Zone.

Wenn Sie in einer Organisationseinheit mit gemischter Verwaltung ein neues Konto einrichten, erhält dieses neue Konto dieselbe (aktualisierte) Regions- und Organisationsstruktur wie die landing zone. Bestehende Konten, die noch nicht aktualisiert wurden, erhalten jedoch nicht den aktualisierten Status der Regionalverwaltung.

Im Allgemeinen kann eine gemischte Governance zu widersprüchlichen oder ungenauen Statusindikatoren in der AWS Control Tower Tower-Konsole führen. Bei gemischter Verwaltung werden Opt-in-Regionen beispielsweise in registrierten Organisationseinheiten für Konten, die noch nicht aktualisiert wurden, mit dem Status Nicht verwaltet angezeigt.

> **Note**
>
> AWS Control Tower erlaubt es nicht, Kontrollen während eines gemischten Governance-Zustands zu aktivieren.

Verhalten von Kontrollen bei gemischter Verwaltung

- Bei gemischter Governance kann AWS Control Tower nicht konsistent Kontrollen bereitstellen, die auf AWS Config Regeln (d. h. detektivische Kontrollen) in Regionen basieren, die in der Organisationseinheit bereits als verwaltet angezeigt werden, da einige Konten in der Organisationseinheit nicht aktualisiert wurden. Möglicherweise erhalten Sie eine `FAILED_TO_ENABLE` Fehlermeldung.
- Wenn Sie bei gemischter Governance die Governance der Landing Zone auf eine Opt-in-Region ausdehnen, während ein Konto in der Organisationseinheit noch nicht aktualisiert wurde, schlägt der `EnableControl` API-Betrieb auf der Organisationseinheit für detektive und proaktive Kontrollen fehl. Sie erhalten eine `FAILED_TO_ENABLE` Fehlermeldung, da nicht aktualisierte

Mitgliedskonten innerhalb der Organisationseinheit noch nicht für diese Regionen zugelassen wurden.

- Bei gemischter Verwaltung, Kontrollen, die Teil des vom Security Hub Service verwalteten Standards sind: AWS Control Tower kann die Einhaltung von Vorschriften in Regionen, in denen eine Diskrepanz zwischen der Konfiguration der landing zone und den Konten besteht, die nicht aktualisiert werden, nicht korrekt melden.
- Eine gemischte Verwaltung ändert nichts am Verhalten von SCP-basierten Kontrollen (präventive Kontrollen), die einheitlich für jedes Konto in einer Organisationseinheit und in jeder kontrollierten Region gelten.

> **Note**
>
> Eine gemischte Unternehmensführung ist nicht dasselbe wie Drift, und sie wird auch nicht als Drift gemeldet.

Um eine gemischte Regierungsführung zu reparieren

- Wählen Sie für jedes Konto in der Organisationseinheit, für das auf der Seite Organizations in der Konsole der Status Update available angezeigt wird, die Option Konto aktualisieren aus.
- Wählen Sie auf der Seite Organizations die Option Organisationseinheit erneut registrieren. Dadurch werden alle Konten in der Organisationseinheit für Organisationseinheiten mit weniger als 300 Konten automatisch aktualisiert.

Überlegungen zur Aktivierung von 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 oder einfach Regionen bezeichnet.

Der Begriff „Opt-In“ hat eine historische Grundlage. Alle Regionen, die nach dem 20. März 2019 AWS-Regionen eingeführt wurden, gelten als Opt-in-Regionen. Für Opt-in-Regionen gelten höhere Sicherheitsanforderungen als für kommerzielle Regionen, was die gemeinsame Nutzung von IAM-Daten über Konten angeht, die in Opt-in-Regionen aktiv sind. Alle über den IAM-Dienst

verwalteten Daten gelten als Identitätsdaten. Dazu gehören 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 landing zone wird in allen ausgewählten Regionen aktiv.

Wenn Sie sich dafür entscheiden, eine Opt-in-Region als Ihre AWS Control Tower Tower-Heimatregion auszuwählen, aktivieren Sie sie zunächst, indem Sie die Schritte unter Region aktivieren befolgen, wenn Sie bei der AWS Management Console angemeldet sind. Wenn Sie Ihre eigenen bestehenden Log Archive- und Audit-Konten aus einer Opt-in-Region verwenden möchten, aktivieren Sie diese Region zunächst 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-south-1
- Region Afrika (Kapstadt), af-south-1
- Region Naher Osten (Bahrain), me-south-1
- Israel (Tel Aviv), il-central-1
- Region Naher Osten (VAE), me-central-1
- Region Europa (Spanien), eu-south-2
- Region Asien-Pazifik (Hyderabad), ap-south-2
- Region Europa (Zürich), eu-central-2
- Region Asien-Pazifik (Melbourne), ap-southeast-4
- Region Kanada West (Calgary), ca-west-1

AWS Control Tower verfügt über einige Kontrollen, die in den Opt-in-Regionen anders funktionieren als in kommerziellen Regionen. Weitere Informationen finden Sie unter Einschränkungen der Kontrolle. Im Folgenden finden Sie einige Überlegungen, die Sie bei der Bereitstellung von Workloads in Opt-in-Regionen berücksichtigen sollten.

> **Regieren oder aktivieren?**
>
> Denken Sie daran, dass die Verwaltung einer Region eine Aktion ist, die Sie in der AWS Control Tower Tower-Konsole auswählen können, sodass die Kontrollen in der Region angewendet werden können. Das Aktivieren oder Deaktivieren 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 Sie sich dafür entscheiden, Opt-in-Regionen zu verwalten, empfehlen wir, keine Ihrer kontrollierten Opt-in-Regionen zu deaktivieren (sich abzumelden), da dies zum Ausfall Ihrer Workloads führen kann. AWS Control Tower erlaubt die Deaktivierung einer regulierten Region nicht von der AWS Control Tower-Konsole aus. Achten Sie jedoch darauf, dass Sie regulierte Regionen nicht von einer Quelle außerhalb von AWS Control Tower deaktivieren, z. B. von der AWS Abrechnungskonsole oder dem AWS SDK.
- Wenn AWS Control Tower die Verwaltung auf eine Opt-in-Region ausdehnt, wird es in allen Mitgliedskonten für die Region aktiviert (Opt-In). Wenn Sie eine Region aus der Verwaltung 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 von einer Quelle außerhalb von AWS Control Tower deaktiviert wurde, z. B. die AWS Abrechnungskonsole oder das SDK. AWS Wir empfehlen Ihnen, Ressourcen aus den Regionen zu entfernen, die Sie deaktiviert haben, da Ihnen sonst unerwartete Abrechnungsgebühren für diese Ressourcen entstehen könnten.
- Wenn Ihre landing zone außer Betrieb genommen wird, bereinigt AWS Control Tower die Ressourcen in allen kontrollierten Regionen, einschließlich der Opt-in-Regionen. AWS Control Tower deaktiviert die Opt-in-Regionen jedoch nicht. Sie können die Opt-in-Regionen als zusätzlichen Schritt nach der Außerbetriebnahme deaktivieren.
- Wenn es sich bei Ihrer Heimatregion um eine Opt-in-Region handelt und Sie beabsichtigen, bestehende Konten als Ihre Log-Archiv- und Audit-Konten zu registrieren, müssen Sie die Opt-in-Region manuell aktivieren, bevor Sie sie als Heimatregion für Ihre landing zone auswählen können. Weitere Informationen finden Sie unter Region aktivieren.

- Wenn AWS Control Tower mit einer Opt-in-Region als Heimatregion eingerichtet ist und Sie den AWS Control Tower Tower-Service von der AWS Konsole in einer anderen Region aus aufrufen, leitet Sie die Konsole nicht automatisch zur Heimatregion weiter.
- Die zugrunde liegende API hat Kapazitätsgrenzen, wodurch sich die Latenz je nach Anzahl der Regionen, Konten und Dienstauslastung von einigen Minuten auf viele Stunden erhöhen kann. Als bewährte Methode sollten Sie sich nur für diejenigen entscheiden, AWS-Regionen in denen Sie Workloads ausführen, und sich jeweils für eine Region anmelden.

Wichtige Einschränkungen in Bezug auf Unternehmensführung und Kontrollen

- Wenn Sie derzeit eine AWS Control Tower aktiviert haben, die in einer Opt-in-Region nicht unterstützt wird, können Sie die AWS Control Tower Tower-Governance nicht auf diese Opt-in-Region ausdehnen, bis die Steuerung in dieser Region unterstützt wird. Weitere Informationen finden Sie unter Einschränkungen der Kontrolle.
- Wenn Sie AWS Control Tower Governance auf eine Opt-in-Region ausdehnen, in der eine bestimmte Kontrolle nicht unterstützt wird, können Sie diese Kontrolle in keiner Region aktivieren, bis die Kontrolle in allen Regionen unterstützt wird, die Sie mit AWS Control Tower verwalten. Weitere Informationen finden Sie unter Einschränkungen der Kontrolle
- Wenn alle 22 kommerziellen Regionen, in denen AWS Control Tower verfügbar ist, aktiviert sind, einschließlich Opt-in-Regionen, wird die Obergrenze für die Anzahl der Konten pro Organisationseinheit (OU) bei der Ausweitung der Governance auf eine OU reduziert. Das Limit liegt bei 220 statt 300 Konten. Diese Reduzierung ist auf StackSet Einschränkungen zurückzuführen. Wenn Sie die Verwaltung auf Organisationseinheiten mit mehr als 220 Konten ausweiten möchten, reduzieren Sie die Anzahl der aktivierten Regionen.

Konfigurieren Sie die Option „Region Deny Control“

AWS Control Tower bietet zwei Regionsverweigerungskontrollen. Wenn ein Steuerelement aktiviert ist, gilt es für die gesamte landing zone. `GRREGIONDENY` Ein anderes Steuerelement kann`CTMULTISERVICEPV1`, sofern aktiviert, für bestimmte von Ihnen angegebene Organisationseinheiten gelten. Weitere Informationen finden Sie unter Zugriff verweigern auf der AWS Grundlage der angeforderten Daten AWS-Region und Steuerung, die auf die Organisationseinheit angewendet wurde.

Die Region verweigert die Kontrolle, `GRREGIONDENY` ist einzigartig, da sie sich auf die gesamte landing zone bezieht und nicht auf eine bestimmte Organisationseinheit. Um die Steuerung „Region

Deny“ zu konfigurieren, rufen Sie die Seite mit den Landingzone-Einstellungen auf und wählen Sie Einstellungen ändern aus.

- Diese Einstellung kann zu einem späteren Zeitpunkt geändert werden.
- Wenn diese Steuerung aktiviert ist, gilt sie für alle registrierten Organisationseinheiten.
- Dieses Steuerelement kann nicht für einzelne Organisationseinheiten konfiguriert werden.

> **Note**
>
> Bevor Sie die Steuerung „Region verweigern“ aktivieren, stellen Sie sicher, dass Sie in diesen Regionen nicht über Ressourcen verfügen, da Sie nach der Anwendung der Steuerung keinen Zugriff mehr auf Ihre Ressourcen haben werden. Solange die Steuerung aktiviert ist, können Sie in den Regionen, in denen der Zugriff verweigert wurde, keine Ressourcen bereitstellen.

Die Region Deny Control verbietet den Zugriff auf AWS Services, basierend auf Ihrer AWS Control Tower Tower-Regionskonfiguration. Sie verweigert den Zugriff auf AWS Regionen mit dem Status Nicht regiert. Die Region Deny Control verweigert auch den Zugriff auf Regionen, in denen AWS Control Tower nicht verfügbar ist. Sie können den Zugriff auf Ihre Heimatregion nicht verweigern. Bestimmte globale AWS Dienste, wie IAM und AWS Organizations, sind von der Sperrung durch die Region ausgenommen. Weitere Informationen finden Sie unter Zugriff verweigern auf AWS Grundlage der angeforderten Daten. AWS-Region

Wenn Sie das Steuerelement aktivieren, gilt es für alle registrierten Organisationseinheiten der obersten Ebene in Ihrer Hierarchie und wird von den Organisationseinheiten übernommen, die sich weiter unten in der Kette befinden. Wenn Sie die Kontrolle entfernen, wird sie für alle registrierten Organisationseinheiten entfernt, alle nicht verwalteten Regionen in AWS Control Tower behalten den Status Nicht reguliert, und Sie können Ressourcen in Regionen außerhalb der Verfügbarkeit von AWS Control Tower bereitstellen.

- Vollständiger Kontrollname: Zugriff verweigern, AWS basierend auf der angeforderten Region AWS
- Beschreibung von Guardrail: Verbietet den Zugriff auf nicht börsennotierte Operationen in globalen und regionalen Diensten außerhalb der angegebenen Regionen.
- Es handelt sich um eine Wahlkontrolle mit präventiver Anleitung.

Die Vorlage für das Region Deny Control SCP finden Sie unter Zugriff verweigern auf AWS Grundlage der AWS-Region in der AWS Control Tower Control-Referenz angeforderten Angaben. Der AWS Control Tower SCP ähnelt dem SCP für AWS Organizations, ist aber nicht identisch.

Sie können die regionalen Service-Endpunkte auf der Seite Regionale Services festlegen.

Überlegungen zur Region Deny Control auf OU-Ebene

Die wichtigste Überlegung bei der Regionsverweigerungssteuerung auf OU-Ebene besteht darin, zu bestimmen, wie sie mit der Regionsverweigerungssteuerung der landing zone interagiert, wenn beide aktiviert sind. Weitere Informationen finden Sie unter Auf die Organisationseinheit angewendete Steuerung zur Verweigerung von Regionen.

Konten in AWS Control Tower bereitstellen und verwalten

Dieses Kapitel enthält einen Überblick und Verfahren für die Bereitstellung und Verwaltung von Mitgliedskonten in Ihrer AWS Control Tower Tower-Landezone.

Es enthält auch eine Übersicht und Verfahren zur Registrierung eines bestehenden AWS Kontos bei AWS Control Tower.

Weitere Informationen zu Konten in AWS Control Tower finden Sie unterÜber uns AWS-Konten in 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**
>
> Sie können bis zu fünf (5) kontobezogene Vorgänge gleichzeitig ausführen, einschließlich Bereitstellung, Aktualisierung und Registrierung.

Methoden der Bereitstellung

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

Standardmäßig werden Mitgliedskonten über Account Factory erstellt, ein konsolenbasiertes Produkt, das Teil des Service Catalog ist. Wenn sich Ihre landing zone nicht im Drift-Zustand befindet, können Sie Create Account als Methode verwenden, um neue Konten von der Konsole aus hinzuzufügen, sowie Konto registrieren, um bestehende AWS Konten bei AWS Control Tower zu registrieren.

Mit Account Factory können Sie Basiskonten bereitstellen, indem Sie sich auf die Standardeinstellungen von AWS Control Tower verlassen. Sie können auch benutzerdefinierte Konten bereitstellen, die die Anforderungen für spezielle Anwendungsfälle erfüllen.

Account Factory Customization (AFC) ist eine Möglichkeit, benutzerdefinierte Konten über die AWS Control Tower Tower-Konsole bereitzustellen und die Anpassung und Bereitstellung Ihrer Konten

zu automatisieren. Es ermöglicht eine konsolenbasierte, automatisierte Bereitstellung nach einigen einmaligen Einrichtungsschritten, wodurch das Schreiben von Skripten oder das Einrichten von Pipelines entfällt. Weitere Informationen finden Sie unter Passen Sie Konten mit Account Factory Customization (AFC) an.

Konsolenbasierte Methoden:

- Über die Account Factory Factory-Konsole, die Teil von ist AWS Service Catalog, für einfache oder benutzerdefinierte Konten. Konten mit Account Factory bereitstellen und verwaltenEinzelheiten und Anweisungen finden Sie hier.
- Über die Funktion Konto registrieren in AWS Control Tower, falls sich Ihre landing zone nicht im Drift-Zustand befindet. Siehe Registrieren Sie ein bestehendes Konto.
- In der AWS Control Tower Tower-Konsole können Sie Account Factory verwenden, um bis zu fünf Konten gleichzeitig zu erstellen, zu aktualisieren oder zu registrieren.

Automatisierte Methoden:

- Lambda-Code: Über das Verwaltungskonto Ihrer AWS Control Tower Tower-Landing Zone unter Verwendung von Lambda-Code und entsprechenden IAM-Rollen. Siehe Automatisierte Kontobereitstellung mit IAM-Rollen.
- Terraform: Von der AWS Control Tower Account Factory for Terraform (AFT), die auf Account Factory und einem GitOps Modell zur Automatisierung der Kontobereitstellung und -aktualisierung basiert. Siehe Bereitstellen von Konten mit AWS Control Tower Account Factory for Terraform (AFT) .
- Account Factory Factory-Anpassung in der AWS Control Tower Tower-Konsole: Nach den Einrichtungsschritten ist für die future Bereitstellung benutzerdefinierter Konten keine zusätzliche Konfiguration oder Pipeline-Wartung erforderlich. Konten werden mithilfe eines AWS Service Catalog Produkts bereitgestellt, das als Blueprint bezeichnet wird. Ein Blueprint kann Vorlagen oder AWS CloudFormation Terraform-Vorlagen verwenden.

> **Note**
>
> AWS CloudFormation Blueprints können Ressourcen für mehrere Regionen bereitstellen. Terraform-Blueprints können Ressourcen nur für eine einzelne Region bereitstellen. Standardmäßig ist dies die Heimatregion.

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. Schritte zur Registrierung eines vorhandenen AWS-Konto mithilfe der AWS Control Tower Tower-Konsole finden Sie unterRegistrieren Sie ein bestehendes Konto.

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.

Für Konten sind Berechtigungen erforderlich

Die Berechtigungen, die für die einzelnen Methoden zur Bereitstellung und Aktualisierung von Konten erforderlich sind, werden jeweils in den einzelnen Abschnitten behandelt. Mit den entsprechenden Benutzergruppenberechtigungen können Anbieter standardisierte Baselines und Netzwerkkonfigurationen für alle Konten in ihrer Organisation festlegen.

> **Note**
>
> Bei der Bereitstellung eines Kontos muss der Kontoanforderer immer über die und die entsprechenden Berechtigungen verfügen. `CreateAccount` `DescribeCreateAccountStatus` Dieser Berechtigungssatz ist Teil der Administratorrolle und wird automatisch vergeben, wenn ein Anforderer die Administratorrolle übernimmt. Wenn

Sie die Erlaubnis zur Bereitstellung von Konten delegieren, müssen Sie diese Berechtigungen möglicherweise direkt für die Kontoanforderer hinzufügen.

Wenn Sie Konten über die AWS Control Tower Tower-Konsole mit Account Factory erstellen, müssen Sie bei einem Konto mit einem IAM-Benutzer angemeldet sein, für den die `AWSServiceCatalogEndUserFullAccess` Richtlinie aktiviert ist, sowie über Berechtigungen zur Verwendung der AWS Control Tower Tower-Konsole verfügen. Sie können nicht als Root-Benutzer angemeldet sein.

Allgemeine Informationen zu den in AWS Control Tower erforderlichen Berechtigungen finden Sie unterVerwendung identitätsbasierter Richtlinien (IAM-Richtlinien) für AWS Control Tower. Informationen zu Rollen und Konten in AWS Control Tower finden Sie unter Rollen und Konten.

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 Verfahren für Mitgliedskonten

Über uns AWS-Konten in 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, einschließlich Ressourcen in Form von Account Factory Factory-Vorlagen und anderen Ressourcen in Ihrer landing zone. Zu diesen Ressourcen können IAM-Rollen, AWS CloudTrail Trails, von Service Catalog bereitgestellte Produkte und IAM Identity Center-Benutzer gehören. AWS Control Tower stellt gemäß den Anforderungen 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.

Überlegungen zur Mitnahme vorhandener Sicherheits- oder Protokollkonten

Bevor ein Konto AWS-Konto als Sicherheits- oder Protokollierungskonto 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 sich jedoch dafür entscheiden, die AWS-Region Ablehnungsfunktion zu aktivieren, verhindert die Regionsverweigerungskontrolle den Zugriff auf Ressourcen in abgelehnten Regionen.

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 in AWS Control Tower. Sie können Mitgliedskonten — einzeln oder nach OU-Gruppen — in AWS Control Tower anzeigen und registrieren, sofern jedes Konto die Voraussetzungen für die Registrierung erfüllt.

Um ein bestimmtes Konto auf der Seite Organisation anzuzeigen, können Sie im Dropdownmenü oben rechts die Option Nur Konten auswählen und dann den Namen Ihres Kontos aus der Tabelle auswählen. Alternativ können Sie den Namen der übergeordneten Organisationseinheit aus der Tabelle auswählen und auf der Detailseite für diese Organisationseinheit eine Liste aller Konten innerhalb dieser Organisationseinheit einsehen.

Auf der Seite Organisation und der Seite mit den Kontodetails können Sie den Status des Kontos sehen. Dabei handelt es sich um einen der folgenden Bundesstaaten:

- Nicht registriert — Das Konto ist Mitglied der übergeordneten Organisationseinheit, wird aber nicht vollständig von AWS Control Tower verwaltet. Wenn die übergeordnete Organisationseinheit registriert ist, unterliegt das Konto den präventiven Kontrollen, die für die registrierte übergeordnete Organisationseinheit konfiguriert wurden. Die detektiven Kontrollen der Organisationseinheit gelten jedoch nicht für dieses Konto. Wenn die übergeordnete Organisationseinheit nicht registriert ist, gelten für dieses Konto keine Kontrollen.
- Registrierung — Das Konto wird von AWS Control Tower verwaltet. Wir stimmen das Konto mit der Kontrollkonfiguration für die übergeordnete Organisationseinheit ab. Dieser Vorgang kann mehrere Minuten pro Kontoressource in Anspruch nehmen.
- Registriert — Das Konto wird durch die für die übergeordnete Organisationseinheit konfigurierten Steuerungen gesteuert. Es wird vollständig von AWS Control Tower verwaltet.
- Registrierung fehlgeschlagen — Das Konto konnte nicht in AWS Control Tower registriert werden. Weitere Informationen finden Sie unter Häufige Ursachen für eine fehlgeschlagene 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 jüngsten 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 OU haben, können Sie die OU erneut registrieren und diese Konten zusammen aktualisieren.

Ressourcen, die in den gemeinsamen Konten erstellt wurden

In diesem Abschnitt werden die Ressourcen angezeigt, die AWS Control Tower in den gemeinsamen Konten 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	audit

AWS Service	Ressourcentyp	Ressourcenname
		log archive
AWS Organizations	Organisationseinheiten	Security Sandbox
AWS Organizations	Service-Kontrollrichtlinien	aws-guardrails-*
AWS CloudFormation	Stacks	AWSControlTowerBP-BASELINE-CLOUDTRAIL-MASTER AWSControlTowerBP-BASELINE-CONFIG-MASTER(in Version 2.6 und höher)

AWS Service	Ressourcentyp	Ressourcenname
AWS CloudFormation	StackSets	AWSControlTowerBP-BASELINE-CLOUDTRAIL(In 3.0 und höher nicht bereitgestellt) AWSControlTowerBP_BASELINE_SERVICE_LINKED_ROLE (Deployed in 3.2 and later) AWSControlTowerBP-BASELINE-CLOUDWATCH AWSControlTowerBP-BASELINE-CONFIG AWSControlTowerBP-BASELINE-ROLES AWSControlTowerBP-BASELINE-SERVICE-ROLES AWSControlTowerBP-SECURITY-TOPICS AWSControlTowerGuardrailAWS-GR-AUDIT-BUCKET-PUBLIC-READ-PROHIBITED AWSControlTowerGuardrailAWS-GR-AUDIT-BUCKET-PUBLIC-WRITE-PROHIBITED AWSControlTowerLoggingResources

AWS Service	Ressourcentyp	Ressourcenname
		AWSControlTowerSecurityResources AWSControlTowerExecutionRole
AWS Service Catalog	Produkt	AWS Control Tower Account Factory
AWS Config	Aggregator	aws-controltower-ConfigAggregatorForOrganizations
AWS CloudTrail	Trail	aws-controltower-BaselineCloudTrail
Amazon CloudWatch	CloudWatch Logs	aws-controltower/CloudTrailLogs
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 AWS 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.

Kontoressourcen protokollieren und archivieren

Wenn Sie Ihre landing zone einrichten, werden die folgenden AWS Ressourcen in Ihrem Logarchivkonto erstellt.

AWS Service	Ressourcentyp	Ressourcenname
AWS CloudFormation	Stacks	StackSet-AWSControlTowerGuardrailAWS-GR-AUDIT-BUCKET-PUBLIC-READ-PROHIBITED- StackSet-AWSControlTowerGuardrailAWS-GR-AUDIT-BUCKET-PUBLIC-WRITE-PROHIBITED StackSet-AWSControlTowerBP-BASELINE-CLOUDWATCH- StackSet-AWSControlTowerBP-BASELINE-CONFIG- StackSet-AWSControlTowerBP-BASELINE-CLOUDTRAIL- StackSet-AWSControlTowerBP-BASELINE-SERVICE-ROLES- StackSet-AWSControlTowerBP-BASELINE-SERVICE-LINKED-ROLE-(In 3.2 and later)

AWS Service	Ressourcentyp	Ressourcenname
		StackSet-AWSControlTowerBP-BASELINE-ROLES- StackSet-AWSControlTowerLoggingResources-
AWS Config	AWS-Config-Regeln	AWSControlTower_AWS-GR_AUDIT_BUCKET_PUBLIC_READ_PROHIBITED AWSControlTower_AWS-GR_AUDIT_BUCKET_PUBLIC_WRITE_PROHIBIT
AWS CloudTrail	Trails	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 AWSControlTowerExecution
AWS Identity and Access Management	Richtlinien	AWSControlTowerServiceRolePolicy
Amazon Simple Notification Service	Themen	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-*

Kontoressourcen prüfen

Wenn Sie Ihre landing zone einrichten, werden die folgenden AWS Ressourcen in Ihrem Auditkonto erstellt.

AWS Service	Ressourcentyp	Ressourcenname
AWS CloudFormation	Stacks	StackSet-AWSControlTowerGuardrailAWS-GR-AUDIT-BUCKET-PUBLIC-READ-PROHIBITED- StackSet-AWSControlTowerGuardrailAWS-GR-AUDIT-BUCKET-PUBLIC-WRITE-PROHIBITED- StackSet-AWSControlTowerBP-BASELINE-CLOUDWATCH- StackSet-AWSControlTowerBP-BASELINE-CONFIG- StackSet-AWSControlTowerBP-BASELINE-CLOUDTRAIL- StackSet-AWSControlTowerBP-BASELINE-SERVICE-ROLES- StackSet-AWSControlTowerBP-BASELINE-SERVICE-LINKED-ROLE-(In 3.2 and later)

AWS Service	Ressourcentyp	Ressourcenname
		StackSet-AWSControlTowerBP-SECURITY-TOPICS- StackSet-AWSControlTowerBP-BASELINE-ROLES- StackSet-AWSControlTowerSecurityResources-*
AWS Config	Aggregator	aws-controltower-GuardrailsComplianceAggregator
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
AWS Identity and Access Management	Richtlinien	AWSControlTowerServiceRolePolicy
Amazon Simple Notification Service	Themen	aws-controltower-AggregateSecurityNotifications aws-controltower-AllConfigNotifications aws-controltower-SecurityNotifications
AWS Lambda	Funktionen	aws-controltower-NotificationForwarder

Über die gemeinsamen Konten

Drei spezielle Konten AWS-Konten sind mit AWS Control Tower verknüpft: das Verwaltungskonto, das Auditkonto und das Protokollarchiv-Konto. Diese Konten werden in der Regel als gemeinsame Konten oder manchmal auch als Kernkonten bezeichnet.

- Sie können benutzerdefinierte Namen für die Audit- und Protokollarchivkonten 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 Sicherheits- oder Protokollierungskonto für AWS Control Tower angeben. Diese Option macht es überflüssig, dass AWS Control Tower neue, gemeinsame Konten erstellt. (Dies ist eine einmalige Auswahl.)

Weitere Informationen zu den gemeinsam genutzten Konten und den zugehörigen Ressourcen finden Sie unterRessourcen, die in den gemeinsamen Konten 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 gemeinsamen Konten erstellt wurden

Protokollarchivkonto

Das gemeinsame Log-Archive-Konto wird automatisch eingerichtet, wenn Sie Ihre landing zone erstellen.

Dieses Konto enthält einen zentralen Amazon S3 S3-Bucket zum Speichern einer Kopie aller Konten AWS CloudTrail und AWS Config Protokolldateien für alle anderen Konten in Ihrer landing zone. Als bewährte Methode empfehlen wir, den Zugriff auf das Protokollarchiv-Konto auf Teams zu beschränken, die für die Einhaltung von Vorschriften und Untersuchungen sowie die entsprechenden Sicherheits- oder Audit-Tools verantwortlich sind. Dieses Konto kann für automatisierte Sicherheitsaudits oder zum Hosten benutzerdefinierter AWS-Config-Regeln Funktionen wie Lambda-Funktionen zur Durchführung von Korrekturmaßnahmen verwendet werden.

> **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-Landezone, Version 3.3.

Weitere Informationen zu den Rollen und Ressourcen, die im Protokollarchiv-Konto verfügbar sind, finden Sie unter Kontoressourcen protokollieren und archivieren

> **Note**
>
> Diese Protokolle können nicht geändert werden. Alle Protokolle werden für Prüfungs- und Compliance-Untersuchungen im Zusammenhang mit Kontoaktivitäten gespeichert.

Prüfungskonto

Dieses gemeinsame Konto wird automatisch eingerichtet, wenn Sie Ihre landing zone erstellen.

Das Auditkonto sollte auf Sicherheits- und Compliance-Teams mit kontenübergreifenden 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 genutzt 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 Prüfkonto erhält auch Benachrichtigungen über den Service Amazon Simple Notification Service (Amazon SNS). Es können drei Kategorien von Benachrichtigungen empfangen werden:

- 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 zu 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. Auf diese Weise können Administratoren Probleme lösen, die ein einzelnes Konto betreffen, und gleichzeitig alle Kontobenachrichtigungen in Ihrem zentralen Auditkonto zusammenfassen. Weitere Informationen finden Sie im Amazon Simple Notification Service-Entwicklerhandbuch.

Weitere Informationen zu den Rollen und Ressourcen, die im Auditkonto verfügbar sind, finden Sie unterKontoressourcen prüfen.

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 Audit-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 Audit-Konto zu erhalten, müssen Sie in jeder E-Mail, die von AWS Control Tower AWS-Region unterstützt wird, den Link Abonnement bestätigen auswählen.

Über Mitgliedskonten

Mitgliedskonten sind die Konten, über die Ihre Benutzer ihre AWS Workloads ausführen. Diese Mitgliedskonten können in Account Factory, von IAM Identity Center-Benutzern mit Administratorrechten in der Service Catalog-Konsole oder mit automatisierten Methoden erstellt werden. Nach der Erstellung existieren diese Mitgliedskonten in einer Organisationseinheit, die in der AWS Control Tower-Konsole erstellt oder bei AWS Control Tower registriert wurde. Weitere Informationen finden Sie in diesen verwandten Themen:

- Konten mit Account Factory bereitstellen und verwalten
- Automatisieren Sie Aufgaben in AWS Control Tower
- AWS Terminologie und Konzepte für Organizations im AWS Organizations Benutzerhandbuch.

Lesen Sie auch Bereitstellen von Konten mit AWS Control Tower Account Factory for Terraform (AFT) .

> **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

Registriere ein vorhandenes AWS-Konto

Sie können AWS Control Tower Governance auf eine bestehende Einzelperson ausdehnen, AWS-Konto wenn Sie sie in einer Organisationseinheit (OU) registrieren, die bereits von AWS Control Tower verwaltet wird. In Frage kommende Konten existieren in nicht registrierten Organisationseinheiten, die Teil derselben AWS Organizations Organisation wie die AWS Control Tower Tower-Organisationseinheit sind.

> **Note**
>
> Sie können ein vorhandenes Konto nur bei der ersten Einrichtung der landing zone als Audit- oder Protokollarchivkonto registrieren.

Richten Sie zuerst einen vertrauenswürdigen Zugriff ein

Bevor Sie ein vorhandenes AWS-Konto Konto bei AWS Control Tower registrieren können, müssen Sie AWS Control Tower die Erlaubnis erteilen, 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, sodass Ihr Stack automatisch für die Konten in Ihrer ausgewählten Organisation bereitgestellt werden AWS CloudFormation kann. Mit diesem vertrauenswürdigen Zugriff führt die `AWSControlTowerExecution` Rolle die Aktivitäten durch, die für die Verwaltung der einzelnen Konten erforderlich sind. Aus diesem Grund müssen Sie diese Rolle jedem Konto hinzufügen, bevor Sie es registrieren.

Wenn der vertrauenswürdige Zugriff aktiviert ist, AWS 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, sodass es Rollen und Berechtigungen auf bestehende Konten anwenden kann, bevor es sie in eine registrierte Organisationseinheit verschiebt, wodurch sie unter Kontrolle gebracht werden.

Weitere Informationen über vertrauenswürdigen Zugriff und AWS CloudFormation StackSets finden Sie unter AWS CloudFormationStackSetsund AWS Organizations.

Was passiert bei der Kontoregistrierung

Während des Registrierungsprozesses führt AWS Control Tower die folgenden Aktionen aus:

- 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 über 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 anhand 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 dem Konto die AWS Config Regeln hinzu, die die AWS Control Tower Detective Controls anwenden.

Konten und Trails auf Organisationsebene CloudTrail

Alle Mitgliedskonten in einer Organisationseinheit unterliegen dem AWS CloudTrail Pfad für die Organisationseinheit, unabhängig davon, ob sie registriert sind oder nicht:

- Wenn Sie ein Konto bei AWS Control Tower registrieren, wird Ihr Konto durch den AWS CloudTrail Trail für die neue Organisation geregelt. Wenn Sie 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.
- Wenn Sie ein Konto in eine registrierte Organisationseinheit verschieben — zum Beispiel über die AWS Organizations Konsole — und das Konto nicht bei AWS Control Tower registrieren, möchten Sie möglicherweise alle verbleibenden Trails auf Kontoebene für das Konto entfernen. Wenn Sie bereits einen CloudTrail Trail bereitgestellt haben, fallen für Sie doppelte Gebühren an. CloudTrail

Wenn du deine landing zone aktualisierst und dich dafür entscheidest, Trails auf Organisationsebene zu deaktivieren, oder wenn deine landing zone älter als Version 3.0 ist, gelten CloudTrail Trails auf Organisationsebene nicht für deine Konten.

Registrierung vorhandener 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 bestehende 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 standardmäßig keine VPC für Konten in Ihrer Organisation unter AWS Control Tower eingerichtet wird. Weitere Informationen finden Sie unter Erstellen Sie ein Konto in AWS Control Tower ohne VPC.

Voraussetzungen für die Registrierung

Diese Voraussetzungen sind erforderlich, bevor Sie ein vorhandenes AWS-Konto bei AWS Control Tower registrieren können:

1. Um eine bestehende Rolle zu registrieren AWS-Konto, muss die `AWSControlTowerExecution` Rolle in dem Konto vorhanden sein, das Sie registrieren. Einzelheiten und Anweisungen finden Sie unter Konto registrieren.
2. Zusätzlich zu der `AWSControlTowerExecution` Rolle muss das bestehende Mitglied, das AWS-Konto Sie registrieren möchten, über die folgenden Berechtigungen verfügen und über die folgenden Vertrauensbeziehungen verfügen. Andernfalls schlägt die Anmeldung fehl.

   Rollenberechtigung: `AdministratorAccess` (AWS verwaltete Richtlinie)

   Rollen-Vertrauensstellung:

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

```
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::Management Account ID:root"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

3. Wir empfehlen, dass das Konto weder über einen AWS Config Konfigurationsrekorder noch über einen Bereitstellungskanal verfügt. Diese können gelöscht oder geändert werden, AWS CLI bevor Sie ein Konto registrieren können. Andernfalls finden Sie unter Konten registrieren mit vorhandenen AWS Config Ressourcen Anweisungen, wie Sie Ihre vorhandenen Ressourcen ändern können.
4. Das Konto, das Sie registrieren möchten, muss in derselben AWS Organizations Organisation wie das AWS Control Tower Tower-Verwaltungskonto existieren. 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 AWS CloudTrail Pfad für die AWS Control Tower Tower-Organisation. Wenn Sie 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.

Registrieren Sie ein bestehendes Konto

Die Funktion Konto registrieren ist in der AWS Control Tower-Konsole verfügbar und ermöglicht die Registrierung vorhandener Konten, AWS-Konten sodass diese von AWS Control Tower verwaltet werden. Weitere Informationen finden Sie unter Ein vorhandenes Konto registrieren. AWS-Konto

Die Funktion Enroll account (Konto anmelden) ist verfügbar, wenn sich Ihre Landing Zone nicht in einem Abweichungsstatus befindet. So zeigen Sie diese Funktion in der Konsole an:

- Navigieren Sie zur Seite Organisation in AWS Control Tower.
- 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 in der gefilterten Tabelle nach dem Kontonamen.
- Folgen Sie den Schritten zur Registrierung eines einzelnen Kontos, wie im Schritte zur Registrierung eines Kontos Abschnitt gezeigt.

> **Note**
>
> Wenn Sie ein vorhandenes Konto registrieren, stellen Sie sicher AWS-Konto, dass Sie die bestehende E-Mail-Adresse verifizieren. Andernfalls kann ein neues Konto erstellt werden.

Bestimmte Fehler erfordern es möglicherweise, dass Sie die Seite aktualisieren und es erneut versuchen. Wenn sich Ihre Landing Zone in einem Abweichungsstatus befindet, können Sie die Funktion Enroll account (Konto anmelden) möglicherweise nicht erfolgreich verwenden. Sie müssen neue Konten über Account Factory einrichten, bis Ihr Problem in der landing zone behoben ist.

Wenn Sie Konten über die AWS Control Tower Tower-Konsole registrieren, müssen Sie bei einem Konto mit einem Benutzer angemeldet sein, für den die `AWSServiceCatalogEndUserFullAccess` Richtlinie aktiviert ist, sowie über Administratorzugriffsberechtigungen für die Nutzung der AWS Control Tower Tower-Konsole verfügen. Sie können nicht als Root-Benutzer angemeldet sein.

Konten, die Sie registrieren, können über die AWS Control Tower Account Factory aktualisiert werden, so wie Sie jedes andere Konto aktualisieren würden. AWS Service Catalog Aktualisierungsverfahren werden im Abschnitt Aktualisierung und Verschiebung von Accountfactory-Konten mit AWS Control Tower oder mit AWS Service Catalog genannt.

Schritte zur Registrierung eines Kontos

Nachdem die AdministratorAccessGenehmigung (Richtlinie) für Ihr bestehendes Konto gilt, gehen Sie wie folgt vor, um das Konto zu registrieren:

Um ein einzelnes Konto bei AWS Control Tower zu registrieren

- Navigieren Sie zur Seite AWS Control Tower Organization.
- Auf der Seite Organisation können Sie bei Konten, die für eine Registrierung in Frage kommen, oben im Abschnitt im Dropdownmenü „Aktionen“ die Option „Registrieren“ auswählen. Bei diesen Konten wird außerdem die Schaltfläche „Konto registrieren“ angezeigt, wenn Sie sie auf der Seite mit den Kontodetails aufrufen.
- 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 registrieren Sie sie
- 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 aufgefordert werden, die `AWSControlTowerExecution` Rolle hinzuzufügen und die Aktion zu bestätigen.
- Wählen Sie „Anmelden“.
- AWS Control Tower beginnt mit der Registrierung und Sie werden zurück zur Seite mit den Kontodetails geleitet.

Häufige Ursachen für eine fehlgeschlagene 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 einer anderen Region, die von AWS Control Tower unterstützt wird, deaktiviert.
- Möglicherweise sind Sie bei einem Konto angemeldet, das dem Account Factory Portfolio hinzugefügt werden muss AWS Service Catalog. Das Konto muss hinzugefügt werden, bevor Sie Zugriff auf Account Factory haben, damit Sie ein Konto bei AWS Control Tower erstellen oder registrieren können. Wenn der entsprechende Benutzer oder die entsprechende Rolle nicht zum Account Factory Factory-Portfolio hinzugefügt wird, erhalten Sie eine Fehlermeldung, wenn Sie versuchen, ein Konto hinzuzufügen. Anweisungen, wie Sie Zugriff auf AWS Service Catalog Portfolios gewähren, finden Sie unter Benutzern Zugriff gewähren.

- Möglicherweise sind Sie als Stammbenutzer angemeldet.
- Das Konto, das Sie registrieren möchten, hat möglicherweise AWS Config Resteinstellungen. Insbesondere kann das Konto über einen Konfigurationsrekorder oder einen Zustellungskanal verfügen. Diese müssen über gelöscht oder geändert werden, AWS CLI bevor Sie ein Konto registrieren können. Weitere Informationen finden Sie unter Registrieren von Konten mit vorhandenen AWS Config Ressourcen und Interaktion mit AWS Control Tower mithilfe von AWS CloudShell.
- Wenn das Konto zu einer anderen Organisationseinheit mit einem Verwaltungskonto gehört, einschließlich einer anderen AWS Control Tower Tower-Organisationseinheit, müssen Sie das Konto in der aktuellen Organisationseinheit kündigen, bevor es einer anderen Organisationseinheit 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 Ressourcenerstellung ohne bestimmte Tags blockieren. In diesem Fall schlägt die Kontobereitstellung oder Registrierung fehl, da AWS Control Tower das Taggen von Ressourcen nicht unterstützt. Wenn Sie Hilfe benötigen, wenden Sie sich an Ihren Kundenbetreuer, oder. AWS 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 in 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 bestehenden Konten und deren Konfigurationen mit AWS Control Tower kompatibel sind, können Sie die im folgenden Abschnitt empfohlenen Best Practices befolgen.

Empfohlen: Sie können ein zweistufiges Konzept für die Kontoregistrierung einrichten

- Verwenden Sie zunächst ein AWS Config Konformitätspaket, um zu bewerten, wie Ihre Konten von einigen AWS Control Tower Tower-Kontrollen betroffen sein könnten. Informationen darüber, wie sich die Registrierung bei AWS Control Tower auf Ihre Konten auswirken kann, finden Sie unter Erweitern der AWS Control Tower Tower-Governance mithilfe von AWS Config Konformitätspaketen.
- 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 Evaluierung für die Einrichtung einer AWS Control Tower Tower-Landezone entscheiden, müssen Sie möglicherweise den AWS Config Lieferkanal und den Konfigurationsrekorder entfernen, die für Ihre Evaluierung erstellt wurden. Dann können Sie AWS Control Tower erfolgreich einrichten.

> **Note**
>
> Das Conformance Pack funktioniert auch in Situationen, in denen sich die Konten in von AWS Control Tower registrierten Organisationseinheiten befinden, die Workloads jedoch in AWS Regionen ausgeführt werden, die keinen AWS Control Tower Tower-Support bieten. Sie können das Conformance Pack verwenden, um Ressourcen in Konten zu verwalten, die in Regionen existieren, in denen AWS Control Tower nicht bereitgestellt wird.

Was ist, 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 Teil derselben Gesamtorganisation sein müssen. Um diese Voraussetzung für die Kontoregistrierung zu erfüllen, können Sie diese vorbereitenden Schritte befolgen, um ein Konto in dieselbe Organisation wie AWS Control Tower zu verschieben.

Vorbereitende Schritte, um ein Konto derselben Organisation wie AWS Control Tower zuzuordnen

1. Löschen Sie das Konto aus der bestehenden Organisation. Wenn Sie diesen Ansatz verwenden, müssen Sie eine separate Zahlungsmethode angeben.

2. Laden Sie das Konto ein, der AWS Control Tower Tower-Organisation beizutreten. Weitere Informationen finden Sie im AWS Organizations Benutzerhandbuch unter Ein AWS Konto zum Beitritt zu Ihrer Organisation einladen.
3. Nehmen Sie die Einladung an. Das Konto wird im Stammverzeichnis der Organisation angezeigt. Durch diesen Schritt wird das Konto in dieselbe Organisation wie AWS Control Tower verschoben und SCPs und konsolidierte Fakturierung eingerichtet.

> **Tip**
>
> Sie können die Einladung für die neue Organisation versenden, bevor das Konto aus der alten Organisation gelöscht wird. Die Einladung wartet, wenn das Konto offiziell aus der bestehenden Organisation austritt.

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 jeden vorhandenen AWS Config Konfigurationsrekorder oder Bereitstellungskanal über das AWS CLI oder AWS CloudShell. Weitere Informationen finden Sie unter Beispiel für AWS Config CLI-Befehle für den Ressourcenstatus und Registrieren von Konten mit vorhandenen 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 Registrierung eines Kontos. Dieser Schritt bringt das Konto in die vollständige AWS Control Tower Tower-Governance.

Optionale Schritte zum Aufheben der Bereitstellung eines Kontos, sodass es registriert werden kann und sein Stack beibehalten werden kann

1. Um den angewendeten AWS CloudFormation Stack beizubehalten, löschen Sie die Stack-Instance aus den Stack-Sets und wählen Sie Stacks beibehalten für die Instance aus.
2. Kündigen Sie das vom Konto bereitgestellte Produkt in AWS Service Catalog Account Factory. (Dieser Schritt entfernt nur das bereitgestellte Produkt aus AWS Control Tower. Das Konto wird dadurch nicht gelöscht.)

3. Richten Sie das Konto mit den erforderlichen Rechnungsdetails ein, wie sie für jedes Konto erforderlich sind, das keiner Organisation gehört. 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 übrig sind, und schließen Sie es dann, nachdem Sie die Schritte zur Kontoschließung unter beschrieben habenDie Verwaltung eines Kontos aufheben.
5. Wenn Sie eine gesperrte Organisationseinheit mit definierten Kontrollen haben, können Sie das Konto dorthin verschieben, anstatt Schritt 1 auszuführen.

Beispiel für AWS Config CLI-Befehle für den Ressourcenstatus

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`

Die normale Antwort ist so etwas wie `"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`*

Fügen Sie die erforderliche IAM-Rolle manuell zu einer vorhandenen hinzu AWS-Konto und registrieren Sie sie

Wenn Sie Ihre AWS Control Tower-Landing landing zone bereits eingerichtet haben, können Sie damit beginnen, die Konten Ihrer Organisation in einer OU zu registrieren, die bei AWS Control Tower registriert ist. Wenn Sie Ihre landing zone noch nicht eingerichtet haben, folgen Sie den Schritten, die im AWS Control Tower Tower-Benutzerhandbuch unter Erste Schritte, Schritt 2 beschrieben sind. Wenn die landing zone fertig ist, führen Sie die folgenden Schritte aus, um bestehende Konten manuell unter die Verwaltung durch AWS Control Tower zu bringen.

Lesen Sie sich unbedingt die zuvor Voraussetzungen für die Registrierung in diesem Kapitel genannten Punkte durch.

Bevor Sie ein Konto bei AWS Control Tower registrieren, müssen Sie AWS Control Tower die Erlaubnis zur Verwaltung dieses Kontos erteilen. 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 erstellt haben AWS Organizations und sich mit einer kontoübergreifenden IAM-Rolle anmelden, 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 die zugehörige Konto-ID.
4. Öffnen Sie das Dropdownmenü für das Konto 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 AWS Management Console als Kind angemeldet sein.
8. Wenn Sie fertig sind, bleiben Sie für den nächsten Teil des Vorgangs im 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. Gehen Sie 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 gezeigte 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:

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
      "Effect":"Allow",
      "Principal":{
         "AWS": "arn:aws:iam::Management Account ID:root"
         },
         "Action": "sts:AssumeRole",
         "Condition": {}
      }
   ]
  }
```

6. Wenn Sie aufgefordert werden, Richtlinien anzuhängen, wählen Sie AdministratorAccess.
7. Wählen Sie Weiter: Tags aus.
8. Möglicherweise wird ein optionaler Bildschirm mit dem Titel Tags hinzufügen angezeigt. Überspringe diesen Bildschirm vorerst, indem du Weiter:Rezension wählst

9. Geben Sie auf dem Überprüfungsbildschirm im Feld Rollenname den Text ein. `AWSControlTowerExecution`
10. Geben Sie in das Feld Beschreibung eine kurze 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. Registrieren Sie das Konto.
   - Wählen Sie auf der Seite Organisation in AWS Control Tower Ihr Konto aus und wählen Sie dann oben rechts im Dropdownmenü Aktionen die Option Registrieren aus.
   - Folgen Sie den Schritten zur Registrierung eines einzelnen Kontos, wie auf der Seite gezeigt. Schritte zur Registrierung eines Kontos
3. Überprüfen Sie die Registrierung.
   - Wählen Sie in AWS Control Tower in der linken Navigationsleiste Organisation aus.
   - Suchen Sie nach dem Konto, das Sie kürzlich registriert haben. Im Anfangsstatus wird der Status „Registrierung“ angezeigt.
   - Wenn sich der Status auf Eingeschrieben ändert, war die Verschiebung 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.

Automatisierte Registrierung von Konten AWS Organizations

Sie können die in einem Blogbeitrag namens Enroll existing AWS accounts into AWS Control Tower beschriebene Registrierungsmethode verwenden, um Ihre AWS Organizations Konten mit einem programmatischen Prozess bei AWS Control Tower zu registrieren.

Die folgende YAML-Vorlage kann Ihnen dabei helfen, die erforderliche Rolle in einem Konto zu erstellen, sodass 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
```

Registrieren von Konten mit vorhandenen AWS Config Ressourcen

Dieses Thema bietet einen step-by-step Ansatz für die Registrierung von Konten mit vorhandenen AWS Config Ressourcen. Beispiele für die Überprüfung Ihrer vorhandenen Ressourcen finden Sie unter Beispiel für AWS Config CLI-Befehle für den Ressourcenstatus.

> **Note**
>
> Wenn Sie vorhandene AWS Konten als Audit- und Protokollarchivkonten in AWS Control Tower einbinden möchten und diese Konten über vorhandene AWS Config Ressourcen

verfügen, müssen Sie die vorhandenen AWS Config Ressourcen vollständig löschen, bevor Sie diese Konten zu diesem Zweck bei AWS Control Tower registrieren können. Für Konten, die nicht zu Audit -und Protokollarchivkonten werden sollen, können Sie die vorhandenen Config-Ressourcen ändern.

Beispiele für - AWS Config Ressourcen

Hier sind einige Arten von AWS Config Ressourcen, die Ihr Konto bereits haben könnte. Diese Ressourcen müssen möglicherweise geändert werden, damit Sie Ihr Konto bei AWS Control Tower registrieren können.

- AWS Config Recorder
- AWS Config Übermittlungskanal
- AWS Config Aggregationsautorisierung

Annahmen

- Sie haben eine Landing Zone von AWS Control Tower 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 AWS Control Tower-Regionen, die durch das Verwaltungskonto geregelt werden.
- Ihr Konto ist nicht das AWS Control Tower-Verwaltungskonto.
- Ihr Konto befindet sich nicht in der Governance-Abweichung.

Einen Blog, der einen automatisierten Ansatz für die 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. Sie können ein einzelnes Support-Ticket für alle Konten einreichen, die Sie registrieren möchten, wie unter beschriebenSchritt 1: Wenden Sie sich mit einem Ticket an den Kundensupport, um das Konto zur Zulassungsliste von AWS Control Tower hinzuzufügen.

Einschränkungen

- Das Konto kann nur mithilfe des AWS Control Tower-Workflows zur Erweiterung der Governance registriert werden.

- Wenn die Ressourcen geändert werden und eine Abweichung für das Konto erstellen, aktualisiert AWS Control Tower die Ressourcen nicht.
- AWS Config -Ressourcen in Regionen, die nicht von AWS Control Tower verwaltet werden, werden nicht geändert.

> **Note**
>
> Wenn Sie versuchen, ein Konto mit vorhandenen Config-Ressourcen zu registrieren, ohne dass das Konto zur Zulassungsliste hinzugefügt wird, 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 in eine andere AWS Control Tower-Organisationseinheit verschieben, führt dies zu einer Governance-Abweichung, wodurch auch verhindert wird, dass das Konto der Zulassungsliste hinzugefügt wird.

Dieser Prozess umfasst 5 Hauptschritte.

1. Fügen Sie das Konto der AWS Control Tower-Zulassungsliste hinzu.
2. Erstellen Sie eine neue IAM-Rolle im Konto.
3. Ändern Sie bereits vorhandene AWS Config Ressourcen.
4. Erstellen Sie AWS Config Ressourcen in AWS Regionen, in denen sie nicht vorhanden sind.
5. Registrieren Sie das Konto bei AWS Control Tower.

Bevor Sie fortfahren, sollten Sie die folgenden Erwartungen an diesen Prozess berücksichtigen.

- AWS Control Tower erstellt keine AWS Config Ressourcen in diesem Konto.
- Nach der Registrierung schützt AWS Control Tower 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, um sie an die AWS Control Tower-Einstellungen anzupassen, bevor Sie das Konto erneut registrieren können.

Schritt 1: Wenden Sie sich mit einem Ticket an den Kundensupport, um das Konto zur Zulassungsliste von AWS Control Tower hinzuzufügen

Fügen Sie diesen Satz in Ihre Ticket-Betreffzeile ein:

Registrieren von Konten mit vorhandenen AWS Config Ressourcen in AWS Control Tower

Fügen Sie die folgenden Details in den Tickettext ein:

- Verwaltungskontonummer
- Kontonummern von Mitgliedskonten, die über vorhandene AWS Config Ressourcen verfügen
- Ihre ausgewählte Heimatregion für die Einrichtung von AWS Control Tower

> **Note**
>
> Die erforderliche Zeit für das Hinzufügen Ihres Kontos zur Zulassungsliste beträgt 2 Werktage.

Schritt 2: Erstellen einer neuen IAM-Rolle im Mitgliedskonto

1. Öffnen Sie die AWS 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 als CustomerCreatedConfigRecorderRoleForControlTower an
4. Erstellen Sie den Stack.

> **Note**
>
> Alle von Ihnen erstellten SCPs sollten eine `-aws-controltower-ConfigRecorderRole*`Rolle ausschließen. Ändern Sie nicht die Berechtigungen, die die Fähigkeit von AWS Config Regeln zur Durchführung von Bewertungen einschränken. Befolgen Sie diese Richtlinien, damit Sie kein erhalten, `AccessDeniedException` wenn Sie SCPs haben, die den Aufruf `aws-controltower-ConfigRecorderRole*` von Config blockieren.

Schritt 3: Identifizieren der AWS Regionen mit bereits vorhandenen Ressourcen

Identifizieren und notieren Sie sich für jede verwaltete Region (von AWS Control Tower verwaltet) im Konto die Regionen, die mindestens einen der zuvor gezeigten vorhandenen AWS Config Ressourcenbeispieltypen haben.

Schritt 4: Identifizieren der AWS Regionen ohne AWS Config Ressourcen

Identifizieren und notieren Sie für jede verwaltete 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 der vorhandenen Ressourcen in jeder AWS Region

Für diesen Schritt werden die folgenden Informationen zu Ihrer AWS Control Tower-Einrichtung benötigt.

- LOGGING_ACCOUNT – die ID des Protokollierungskontos
- AUDIT_ACCOUNT – die Audit-Konto-ID
- IAM_ROLE_ARN – der in Schritt 1 erstellte IAM-Rollen-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 den Anweisungen in den Abschnitten 5a bis 5c folgen.

Schritt 5a. AWS Config Recorder-Ressourcen

Pro AWS Region kann nur ein AWS Config Recorder vorhanden sein. Wenn eine vorhanden ist, ändern Sie die Einstellungen wie gezeigt. Ersetzen Sie das Element in Ihrer Heimatregion GLOBAL_RESOURCE_RECORDING durch „true“. Ersetzen Sie das Element für andere Regionen, in denen ein - AWS Config Recorder vorhanden ist, durch false.

- 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 Recorder-Namen.

```
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. Ändern der Ressourcen des AWS Config Übermittlungskanals

Pro Region kann nur ein AWS Config Übermittlungskanal vorhanden sein. Wenn ein anderes vorhanden ist, ändern Sie die Einstellungen wie gezeigt.

- Name: NICHT ÄNDERN
- ConfigSnapshotDeliveryProperties: TwentyFour_Stunden
- S3BucketName: Der Name des Protokoll-Buckets aus dem AWS Control Tower-Protokollierungskonto

  `aws-controltower-logs-LOGGING_ACCOUNT-HOME_REGION`
- S3KeyPrefix: *ORGANIZATION_ID*
- SnsTopicARN: Der ARN des SNS-Themas aus dem Audit-Konto im 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 Recorder-Namen.

```
aws configservice put-delivery-channel --delivery-channel
 name=DELIVERY_CHANNEL_NAME,s3BucketName=aws-controltower-
logs-LOGGING_ACCOUNT_ID-
HOME_REGION,s3KeyPrefix="ORGANIZATION_ID",configSnapshotDeliveryProperties={deliveryFrequency=T
controltower-AllConfigNotifications --region CURRENT_REGION
```

Schritt 5c. Ändern von Ressourcen für die AWS Config Aggregationsautorisierung

Pro Region können mehrere Aggregationsautorisierungen vorhanden sein. AWS Control Tower erfordert eine Aggregationsautorisierung, die das Auditkonto als autorisiertes Konto angibt und die Heimatregion für AWS Control Tower als autorisierte Region hat. Wenn es nicht existiert, erstellen Sie eine neue mit den folgenden Einstellungen:

- AuthorizedAccountId: Die Audit-Konto-ID

- AuthorizedAwsRegion: Die Heimatregion für die AWS Control Tower-Einrichtung

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: Erstellen von Ressourcen, in denen sie nicht vorhanden sind, in Regionen, die von AWS Control Tower verwaltet werden

Überarbeiten Sie die AWS CloudFormation Vorlage, sodass in Ihrer Heimatregion der IncludeGlobalResourcesTypes Parameter den Wert hat`GLOBAL_RESOURCE_RECORDING`, wie im folgenden Beispiel gezeigt. Aktualisieren Sie auch die erforderlichen Felder in der Vorlage, wie in diesem Abschnitt angegeben.

Ersetzen Sie das Element in Ihrer Heimatregion `GLOBAL_RESOURCE_RECORDING` durch „true“. Ersetzen Sie das Element für andere Regionen, in denen ein - AWS Config Recorder vorhanden ist, durch false.

1. Navigieren Sie zur AWS CloudFormation Konsole des Verwaltungskontos.
2. Erstellen Sie einen neuen StackSet mit dem Namen CustomerCreatedConfigResourcesForControlTower.
3. Kopieren und aktualisieren Sie die folgende Vorlage:

```
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: aws-controltower-logs-LOGGING_ACCOUNT-HOME_REGION
      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 im Feld S3BucketName die Felder *LOGGING_ACCOUNT_ID* und *HOME_REGION*

b. Ersetzen Sie im Feld S3KeyPrefix die *ORGANIZATION_ID*

c. Ersetzen Sie im Feld SnsTopicARN den *AUDIT_ACCOUNT*

d. Ersetzen Sie im AuthorizedAccountId Feld *AUDIT_ACCOUNT*

e. Ersetzen Sie im AuthorizedAwsRegion Feld die Option *HOME_REGION*

4. Fügen Sie während der Bereitstellung in der AWS 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 der Organisationseinheit bei AWS Control Tower

Registrieren Sie im AWS Control Tower-Dashboard die Organisationseinheit.

> **Note**
>
> Der Workflow Konto registrieren ist für diese Aufgabe nicht erfolgreich. Sie müssen OU registrieren oder OU erneut registrieren wählen.

Konten mit Account Factory bereitstellen und verwalten

Dieses Kapitel enthält einen Überblick und Verfahren für die Bereitstellung neuer Mitgliedskonten in einer AWS Control Tower Tower-Landezone mit Account Factory.

Berechtigungen für die Konfiguration und Bereitstellung von Konten

Die AWS Control Tower Account Factory ermöglicht Cloud-Administratoren und Benutzern AWS IAM Identity Center die Bereitstellung von Konten in Ihrer landing zone. 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, so wie Sie es tun würden, wenn Sie ein Konto verwenden würden, das über Berechtigungen in Ihrer gesamten Organisation verfügt.

Das AWS Control Tower 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 AWS-Konto vorhandenes Konto bei AWS Control Tower zu registrieren, muss die `AWSControlTowerExecution` Rolle für dieses Konto aktiviert sein. Weitere Informationen zum Registrieren eines vorhandenen Kontos finden Sie unter Registriere ein vorhandenes AWS-Konto.

Weitere Informationen zu Berechtigungen finden Sie unter Für Konten sind Berechtigungen erforderlich.

Konten mit AWS Service Catalog Account Factory bereitstellen

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 Konten möglicherweise programmgesteuert, mit der AWS CLI 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.

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 Management Console 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:

   - Das SSO UserEmail kann eine neue E-Mail-Adresse oder die E-Mail-Adresse sein, 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 SSO eine neue E-Mail-Adresse verwendet habenUserEmail, 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.

Überlegungen zur Verwaltung von Konten in Account Factory

Sie können Konten, die Sie über Account Factory erstellt und bereitgestellt haben, aktualisieren, deren Verwaltung aufheben und schließen. Sie können Konten wiederverwenden, indem Sie die Benutzerparameter in den Konten aktualisieren, die Sie wiederverwenden möchten. Sie können auch die Organisationseinheit (OU) eines Kontos ändern.

> **Note**
>
> Wenn Sie ein bereitgestelltes Produkt aktualisieren, das mit einem Konto verknüpft ist, das Account Factory verkauft, erstellt AWS Control Tower einen neuen Benutzer im IAM Identity Center AWS IAM Identity Center, wenn Sie eine neue Benutzer-E-Mail-Adresse angeben. Das zuvor erstellte Konto wird nicht entfernt. Informationen zum Entfernen der E-Mail-Adresse des vorherigen IAM Identity Center-Benutzers aus IAM Identity Center finden Sie unter Benutzer deaktivieren.

Aktualisierung und Verschiebung von Accountfactory-Konten mit AWS Control Tower oder mit AWS Service Catalog

Am einfachsten können Sie ein registriertes Konto über die AWS Control Tower Tower-Konsole aktualisieren. Individuelle Kontoaktualisierungen sind nützlich, um Abweichungen zu beheben, wie z. Moved Member Account (Mitgliedskonto verschoben) Im Rahmen eines vollständigen landing zone Zone-Updates sind auch Kontoaktualisierungen erforderlich.

Wenn Sie ein Konto von einer Organisationseinheit (OU) in eine andere verschieben, denken Sie daran, dass sich die von der neuen Organisationseinheit angewandten Kontrollen möglicherweise von den Kontrollen in der vorherigen Organisationseinheit unterscheiden. Stellen Sie sicher, dass die Kontrollen in der neuen Organisationseinheit Ihren Richtlinienanforderungen für das Konto entsprechen.

Steuern Sie das Verhalten, wenn Konten zwischen Konten verschoben werden Organisationseinheiten

Wenn Sie ein Konto zwischen Organisationseinheiten verschieben, werden die Steuerelemente für die Ziel-Organisationseinheit auf die Konto. Die Kontrollen, die von der früheren Organisationseinheit für das Konto galten, sind jedoch nicht entfernt. Das genaue Verhalten der Steuerelemente ist spezifisch für die Implementierung von Steuerelemente, die auf der ehemaligen Organisationseinheit und der Zielorganisationseinheit aktiv sind.

- Für Steuerelemente, die mit AWS Config Regeln implementiert wurden: Die Steuerelemente aus der vorherigen Organisationseinheit werden nicht entfernt. Diese Steuerelemente müssen manuell entfernt werden.
- Für mit SCPs implementierte Kontrollen: Die SCP-basierten Kontrollen aus der vorherigen Organisationseinheit sind entfernt. Die SCP-basierten Kontrollen für die Ziel-OU treten für dieses Konto in Kraft.
- Für Steuerungen, die mit AWS CloudFormation Hooks implementiert wurden: Dieses Verhalten hängt vom Status der Steuerelemente in der neuen Organisationseinheit ab.
  - Wenn in der Ziel-Organisationseinheit keine Hook-basierten Steuerungen aktiv sind: Die alte Die Steuerelemente bleiben für das verschobene Konto 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.

Aktualisieren Sie das Konto in der Konsole

Um ein Konto in der AWS Control Tower Tower-Konsole zu aktualisieren

1. Wenn Sie bei AWS Control Tower angemeldet sind, navigieren Sie zur Organisationsseite.
2. Wählen Sie in der Liste der Organisationseinheiten und Konten den Namen des Kontos aus, das Sie aktualisieren möchten. Für Konten, die zur Aktualisierung verfügbar sind, wird der Status Update verfügbar angezeigt.
3. Als Nächstes sehen Sie die Seite mit den Kontodetails für Ihr ausgewähltes Konto.
4. Wählen Sie oben rechts die Option Konto aktualisieren aus.

Aktualisieren Sie das bereitgestellte Produkt

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.

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:

      - SSO UserEmail (in den bereitgestellten Produktdetails verfügbar)
      - AccountEmail(In den bereitgestellten Produktdetails verfügbar)
      - SSO UserFirstName (verfügbar im IAM Identity Center)
      - SSOU SerLastName (im IAM Identity Center verfügbar)
      - 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.

Ändern Sie die E-Mail-Adresse eines registrierten Kontos

Gehen Sie wie in diesem Abschnitt beschrieben vor, um die E-Mail-Adresse eines registrierten Mitgliedskontos in AWS Control Tower zu ändern.

> **Note**
>
> Das folgende Verfahren erlaubt es Ihnen nicht, die E-Mail-Adresse eines Verwaltungskontos, eines Protokollarchiv-Kontos oder eines Audit-Kontos zu ändern. Weitere Informationen dazu finden Sie unter Wie ändere ich die mit meinem AWS Konto verknüpfte E-Mail-Adresse? oder wenden Sie sich an AWS den Support.

Um die E-Mail-Adresse eines Kontos zu ändern, das AWS Control Tower erstellt

1. Stellen Sie das Root-Benutzerpasswort für das Konto wieder her. Sie können den Schritten im Artikel Wie kann ich ein verlorenes oder vergessenes AWS Passwort wiederherstellen? folgen
2. Melden Sie sich mit dem Root-Benutzerpasswort bei dem Konto an.
3. Ändern Sie die E-Mail-Adresse wie jede andere E-Mail-Adresse und warten Sie AWS-Konto, bis sich die Änderung bemerkbar macht AWS Organizations. Es kann zu Verzögerungen kommen, bis die Änderung der E-Mail-Adresse vollständig aktualisiert ist.
4. Aktualisieren Sie das bereitgestellte Produkt im Service Catalog mit der E-Mail-Adresse, die zuvor zu dem Konto gehörte. Der Prozess zur Aktualisierung des bereitgestellten Produkts

umfasst die Verknüpfung der neuen E-Mail-Adresse mit dem bereitgestellten Produkt. Auf diese Weise wird die Änderung der E-Mail-Adresse in AWS Control Tower wirksam. Verwenden Sie die neue E-Mail-Adresse für Updates zu anschließend bereitgestellten Produkten.

Informationen zum Ändern des Kennworts oder der E-Mail-Adresse eines Mitgliedskontos, mit dem Sie es erstellt haben AWS Organizations, finden Sie im Benutzerhandbuch unter Zugreifen auf ein Mitgliedskonto als AWS Organizations Root-Benutzer.

Ändern Sie den Namen eines registrierten Kontos

Gehen Sie wie in diesem Abschnitt beschrieben vor, um den Namen eines registrierten AWS Control Tower 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

1. Stellen Sie das Root-Passwort für das Konto wieder her. Sie können die in diesem Artikel beschriebenen Schritte ausführen. Wie stelle ich ein verlorenes oder vergessenes AWS Passwort wieder her?
2. Melden Sie sich mit dem Root-Passwort bei dem Konto an.
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. AWS Control Tower aktualisiert sich automatisch, um die Namensänderung widerzuspiegeln. Dieses Update wird sich nicht auf das bereitgestellte Produkt auswirken. AWS Service Catalog

Account Factory mit den Amazon Virtual Private Cloud Cloud-Einstellungen konfigurieren

Mit Account Factory können Sie vorab genehmigte Baselines 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 Factory-Seite finden Sie eine Liste der Organisationseinheiten (OUs) und deren Status auf der Zulassungsliste. Standardmäßig werden alle OUs auf die Whitelist gesetzt. Dies bedeutet, dass Konten unter ihnen bereitgestellt werden können. Sie können bestimmte Organisationseinheiten 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.

So konfigurieren Sie die Amazon VPC-Einstellungen in Account Factory

1. Melden Sie sich als zentraler Cloud-Administrator mit Administratorrechten im Verwaltungskonto bei der AWS Control Tower 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 und sehen Sie sich die bearbeitbare Version Ihrer Account Factory Factory-Netzwerkkonfigurationseinstellungen an.
3. Sie können jedes Feld der Standardeinstellungen nach Bedarf ändern. Wählen Sie die VPC-Konfigurationsoptionen aus, die Sie für alle neuen Account Factory Factory-Konten einrichten möchten, die Ihre Endbenutzer erstellen können, 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 von privaten Subnetzen in Amazon VPC aus der Liste aus. Standardmäßig ist 1 ausgewählt. Die maximal zulässige Anzahl von privaten Subnetzen beträgt 2 pro Availability Zone.
- 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.

Die Verwaltung eines Kontos aufheben

Wenn Sie ein Konto in Account Factory erstellt oder eines registriert haben und Sie nicht mehr möchten AWS-Konto, dass das Konto von AWS Control Tower in einer landing zone verwaltet wird, können Sie die Verwaltung des Kontos über die AWS Control Tower Tower-Konsole aufheben.

Wenn Sie die Verwaltung eines AWS Control Tower-Kontos aufheben, werden alle von AWS Control Tower bereitgestellten Ressourcen entfernt, einschließlich aller Blueprints. Das Konto wird aus einer beliebigen AWS Control Tower Tower-Organisationseinheit in den Stammbereich 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.

Die Verwaltung eines Kontos kann auch von einem IAM Identity Center-Benutzer in der `AWSAccountFactory` Gruppe in der Service Catalog-Konsole aufgehoben werden, indem er das bereitgestellte Produkt beendet. 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 die Verwaltung eines Mitgliedskontos im Service Catalog aufheben.

So heben Sie die Verwaltung eines registrierten Kontos 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 nicht verwaltet wurde, ändert sich sein Status in Nicht registriert.
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

Wenn Sie die Verwaltung eines benutzerdefinierten Kontos aufheben, entfernt AWS Control Tower die Ressourcen, die der Blueprint bereitgestellt hat, sowie alle anderen Ressourcen, die AWS Control Tower innerhalb des Kontos erstellt hat. Nachdem Sie die Verwaltung des Kontos aufgehoben haben, können Sie das Konto über schließen. AWS Organizations

> **Note**
>
> Ein nicht verwaltetes Konto wird nicht geschlossen oder gelöscht. Wenn das Konto nicht verwaltet 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 in 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 Aktualisierung und Verschiebung von Accountfactory-Konten mit AWS Control Tower oder mit AWS Service Catalog.

Video-Anleitung

In diesem Video (3:25) wird beschrieben, wie Sie ein Konto aus dem AWS Control Tower entfernen, Root-Zugriff auf das Konto erhalten und schließlich das AWS-Konto schließen. 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.

Video-Komplettlösung zum Schließen eines Kontos in AWS Control Tower.

Sie können sich eine Liste von AWS YouTube Videos ansehen, in denen allgemeine Aufgaben in AWS Control Tower erklärt werden.

Schließen Sie ein in Account Factory erstelltes Konto

In Account Factory erstellte Konten sind AWS-Konten. Informationen zum Schließen AWS-Konten finden Sie im Referenzhandbuch zur AWS Kontoverwaltung unter Schließen eines Kontos.

> **Note**
>
> Das Schließen eines AWS-Konto ist nicht dasselbe wie das Aufheben der Verwaltung eines Kontos über den AWS Control Tower — dies sind separate Aktionen. Sie müssen die Verwaltung des Kontos aufheben, bevor Sie es schließen können.

Schließen Sie ein AWS Control Tower Tower-Mitgliedskonto über AWS Organizations

Sie können Ihre AWS Control Tower Tower-Mitgliedskonten über das Verwaltungskonto Ihrer Organisation schließen, ohne dass Sie sich bei jedem Mitgliedskonto einzeln mit Root-Anmeldeinformationen anmelden müssen, und zwar mit Hilfe von AWS Organizations. Sie können Ihr Verwaltungskonto auf diese Weise jedoch nicht schließen.

Wenn Sie die AWS Organizations CloseAccountAPI aufrufen oder ein Konto in der AWS Organizations Konsole schließen, ist das Mitgliedskonto wie jedes andere Konto 90 Tage AWS-Konto lang isoliert. Das Konto zeigt in AWS Control Tower den Status Gesperrt und AWS Organizations. Wenn Sie während dieser 90 Tage versuchen, mit dem Konto zu arbeiten, gibt AWS Control Tower eine Fehlermeldung aus.

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.

Als bewährte Methode empfehlen wir, die Verwaltung eines Mitgliedskontos aufzuheben, bevor Sie dieses Konto schließen. Wenn Sie ein Mitgliedskonto schließen, ohne es zuvor zu deaktivieren, zeigt AWS Control Tower den Status des Kontos als Gesperrt, aber auch als Registriert an. Wenn Sie versuchen, die Organisationseinheit des Kontos während dieser 90 Tage erneut zu registrieren, gibt AWS Control Tower daher 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 die OU erneut registrieren, es AWS kann jedoch zu einem Fehler bezüglich einer fehlenden Zahlungsmethode für das Konto kommen. Um diese Einschränkung zu umgehen, erstellen Sie eine weitere Organisationseinheit und verschieben Sie das Konto in diese Organisationseinheit, bevor Sie versuchen, sich erneut zu registrieren. Wir empfehlen, diese Organisationseinheit „Gesperrte Organisationseinheit“ zu nennen.

> **Note**
>
> Wenn Sie die Verwaltung des Kontos nicht aufheben, 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 CloseAccount API.

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-* StackSet-AWSControlTowerBP-BASELINE-CLOUDWATCH-*

AWS Dienst	Ressourcentyp	Ressourcenname
		StackSet-AWSControlTowerBP-BASELINE-CONFIG-* StackSet-AWSControlTowerBP-BASELINE-ROLES-* StackSet-AWSControlTowerBP-BASELINE-SERVICE-ROLES-*
AWS CloudTrail	Trail	aws-controltower-BaselineCloudTrail
Amazon CloudWatch	CloudWatch Regeln für Veranstaltungen	aws-controltower-ConfigComplianceChangeEventRule
Amazon CloudWatch	CloudWatch Logs	aws-controltower/CloudTrailLogs /aws/lambda/aws-controltower-NotificationForwarder

AWS Dienst	Ressourcentyp	Ressourcenname
AWS Identity and Access Management	Rollen	aws-controltower-AdministratorExecutionRole aws-controltower-CloudWatchLogsRole aws-controltower-ConfigRecorderRole aws-controltower-ForwardSnsNotificationRole aws-controltower-ReadOnlyExecutionRole AWSControlTowerExecution
AWS Identity and Access Management	Richtlinien	AWSControlTowerServiceRolePolicy
Amazon Simple Notification Service	Themen	aws-controltower-SecurityNotifications
AWS Lambda	Anwendungen	StackSet-AWSControlTowerBP-BASELINE-CLOUDWATCH-*
AWS Lambda	Funktionen	aws-controltower-NotificationForwarder

Passen Sie Konten mit Account Factory Customization (AFC) an

Mit AWS Control Tower können Sie neue und bestehende Ressourcen anpassen, AWS-Konten wenn Sie deren Ressourcen über die AWS Control Tower Tower-Konsole bereitstellen. Nachdem Sie die werkseitige Anpassung des Kontos eingerichtet haben, automatisiert AWS Control Tower diesen Prozess für die future Bereitstellung, sodass Sie keine Pipelines verwalten müssen.

Maßgeschneiderte Konten können unmittelbar nach der Bereitstellung der Ressourcen verwendet werden.

Ihre benutzerdefinierten Konten werden in Account Factory, über AWS 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. Vordefinierte Blueprints, die von AWS Partnern erstellt und verwaltet werden, sind ebenfalls verfügbar. Weitere Informationen zu von Partnern verwalteten Blueprints finden Sie in der Bibliothek „Erste Schritte“.AWS Service Catalog

> **Note**
>
> AWS Control Tower enthält proaktive Kontrollen, die AWS CloudFormation Ressourcen im AWS Control Tower überwachen. Optional können Sie diese Steuerungen in Ihrer landing zone aktivieren. Wenn Sie proaktive Kontrollen anwenden, wird überprüft, ob die Ressourcen, die Sie für Ihre Konten bereitstellen möchten, den Richtlinien und Verfahren Ihres Unternehmens entsprechen. Weitere Informationen zu proaktiven Kontrollen finden Sie unter Proaktive Kontrollen.

Ihre Konto-Blueprints werden in einem Konto 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 eine Blaupause, um es von allen anderen Service Catalog-Produkten zu unterscheiden. Weitere Informationen zum Erstellen von Service Catalog-Produkten finden Sie unter Produkte erstellen im AWS Service Catalog Administratorhandbuch.

Wenden Sie Blueprints auf bestehende Konten an

Sie können benutzerdefinierte Blueprints auch auf bestehende Konten anwenden, indem Sie die Schritte Konto aktualisieren in der AWS Control Tower Tower-Konsole befolgen. Details hierzu finden Sie unter Aktualisieren Sie das Konto in der Konsole.

> **Bevor Sie beginnen**
>
> Bevor Sie mit der Erstellung benutzerdefinierter Konten bei AWS Control Tower Account Factory beginnen, müssen Sie eine AWS Control Tower-Landing Zone-Umgebung bereitgestellt haben und Sie müssen eine Organisationseinheit (OU) bei AWS Control Tower registriert haben, in der Ihre neu erstellten Konten platziert werden.

Weitere Informationen zur Arbeit mit AFC finden Sie unter Automatisieren der Kontoanpassung mithilfe von Account Factory Customization in AWS Control Tower.

Vorbereitung für die Anpassung

- Sie können ein neues Konto erstellen, das als Hub-Konto dient, oder Sie können ein vorhandenes verwenden AWS-Konto. Wir empfehlen dringend, das AWS Control Tower Tower-Managementkonto nicht als Ihr Blueprint-Hub-Konto zu verwenden.
- Wenn Sie sich bei AWS Control Tower registrieren AWS-Konten und sie anpassen möchten, müssen Sie die `AWSControlTowerExecution` Rolle zunächst zu diesen Konten hinzufügen, wie Sie es für jedes andere Konto tun würden, das Sie bei AWS Control Tower registrieren.
- Wenn Sie planen, Partner-Blueprints zu verwenden, für die Marketplace-Abonnementanforderungen gelten, müssen Sie diese über Ihr AWS Control Tower Tower-Managementkonto konfigurieren, bevor Sie die Partner-Blueprints als Blueprints für die werkseitige Anpassung von Konten bereitstellen.

Themen

- Für die Anpassung eingerichtet
- Erstellen Sie ein benutzerdefiniertes Konto anhand eines Blueprints
- Registrieren Sie Konten und passen Sie sie an
- Einen Blueprint zu einem AWS Control Tower Tower-Konto hinzufügen
- Aktualisieren Sie einen Blueprint
- Entfernen Sie einen Blueprint aus einem Konto
- Blueprints von Partnern
- Überlegungen zu Account Factory Factory-Anpassungen (AFC)
- Im Falle eines Blueprint-Fehlers
- Anpassen Ihres Richtliniendokuments für AFC-Blueprints auf der Grundlage von CloudFormation
- Zusätzliche Berechtigungen sind für die Erstellung eines Terraform-basierten Service Catalog-Produkts erforderlich

Für die Anpassung eingerichtet

In den nächsten Abschnitten werden Schritte zur Einrichtung von Account Factory für den Anpassungsprozess beschrieben. Wir empfehlen, dass Sie einen delegierten Administrator für das Hub-Konto einrichten, bevor Sie mit diesen Schritten beginnen.

Übersicht

- Schritt 1. Erstellen Sie die erforderliche Rolle. Erstellen Sie eine IAM-Rolle, die AWS Control Tower die Erlaubnis erteilt, Zugriff auf das (Hub-) Konto zu erhalten, 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 „Blueprint-Produkt“ genannt), 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 individuelles Konto zu erstellen. Geben Sie bei der Kontoerstellung die Blueprint-Produktinformationen und die Rolleninformationen in die entsprechenden Felder in Account Factory in der AWS Control Tower Tower-Konsole ein.

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 diese Rolle übernommen wird, gewährt sie AWS Control Tower Zugriff zur Verwaltung des Hub-Kontos. Die Rolle muss benannt AWSControlTowerBlueprintAccesswerden.

AWS Control Tower übernimmt diese Rolle, um in Ihrem Namen eine Portfolio-Ressource zu erstellen AWS Service Catalog, anschließend 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 erläutert.

> Navigieren Sie zur IAM-Konsole, um die erforderliche Rolle einzurichten.

So richten Sie die Rolle in einem registrierten AWS Control Tower Tower-Konto ein

1. Verbinden Sie das AWS Control Tower Tower-Verwaltungskonto oder melden Sie sich als Principal an.
2. Nehmen Sie vom Verbundprinzipal im Verwaltungskonto die Rollen an oder wechseln Sie zu der `AWSControlTowerExecution` Rolle im registrierten AWS Control Tower Tower-Konto, das Sie als Blueprint-Hub-Konto auswählen.
3. Erstellen Sie aus der `AWSControlTowerExecution` Rolle im registrierten AWS Control Tower Tower-Konto die `AWSControlTowerBlueprintAccess` Rolle mit den richtigen Berechtigungen und Vertrauensbeziehungen.

> **Note**
>
> Um den Richtlinien für AWS bewährte Verfahren zu entsprechen, ist es wichtig, dass Sie sich unmittelbar nach der Erstellung 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 annehmen, bevor Sie mit der Einrichtung der `AWSControlTowerBlueprintAccess` Rolle fortfahren.

Um die Rolle in einem nicht registrierten Mitgliedskonto einzurichten

1. Verbinden Sie das Konto, das Sie als Hub-Konto festlegen möchten, oder melden Sie sich mit Ihrer bevorzugten Methode als Hauptbenutzer an.
2. Wenn Sie als Hauptbenutzer im Konto angemeldet sind, erstellen Sie die `AWSControlTowerBlueprintAccess` Rolle mit den entsprechenden Berechtigungen und Vertrauensbeziehungen.

Die AWSControlTowerBlueprintAccessRolle muss so eingerichtet sein, dass sie zwei Prinzipalen Vertrauen gewährt:

- Der Principal (Benutzer), der AWS Control Tower im AWS Control Tower Tower-Verwaltungskonto ausführt.
- Die `AWSControlTowerAdmin` im AWS Control Tower Tower-Verwaltungskonto angegebene Rolle.

Hier ist ein Beispiel für eine Vertrauensrichtlinie, ähnlich einer, die Sie für Ihre Rolle angeben müssen. Diese Richtlinie veranschaulicht die bewährte Methode zur Gewährung des Zugriffs mit den geringsten Rechten. Wenn Sie Ihre eigene Richtlinie erstellen, ersetzen Sie den Begriff *`YourManagementAccountId`*durch die tatsächliche Konto-ID Ihres AWS Control Tower Tower-Verwaltungskontos und ersetzen Sie den Begriff *`YourControlTowerUserRole`*durch die ID der IAM-Rolle für Ihr Verwaltungskonto.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": [
                "arn:aws:iam::YourManagementAccountId:role/service-role/
AWSControlTowerAdmin",
                "arn:aws:iam::YourManagementAccountId:role/YourControlTowerUserRole"
                ]
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

Richtlinie für erforderliche Berechtigungen

AWS Control Tower erfordert, dass die angegebene verwaltete Richtlinie an die `AWSControlTowerBlueprintAccess` Rolle angehängt werden `AWSServiceCatalogAdminFullAccess` muss. Diese Richtlinie bietet Berechtigungen, mit AWS Service Catalog denen 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.

Zusätzliche Berechtigungen können erforderlich sein

- Wenn Sie Ihre Blueprints in Amazon S3 speichern, benötigt AWS Control Tower auch die `AmazonS3ReadOnlyAccess` Berechtigungsrichtlinie für die `AWSControlTowerBlueprintAccess` Rolle.
- Für den Produkttyp AWS Service Catalog Terraform müssen Sie der benutzerdefinierten AFC-IAM-Richtlinie einige zusätzliche Berechtigungen hinzufügen, wenn Sie nicht die standardmäßige Admin-Richtlinie 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 das Produkt AWS Service Catalog

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

Als Ergebnis der HashiCorp aktualisierten Terraform-Lizenzierung wurde die Unterstützung für Terraform Open Source-Produkte und bereitgestellte Produkte auf einen neuen Produkttyp namens External AWS Service Catalog umgestellt. Weitere Informationen darüber, wie sich diese Änderung auf AFC auswirkt, einschließlich der Aktualisierung Ihrer bestehenden Konto-Blueprints auf den Produkttyp Extern, finden Sie unter Übergang zum externen Produkttyp.

Zusammenfassung der Schritte zur Erstellung eines Blueprints

- Erstellen Sie eine AWS CloudFormation Vorlage oder eine Terraform-Konfigurationsdatei tar.gz, die zu Ihrem Konto-Blueprint wird, oder laden Sie sie herunter. Einige Vorlagenbeispiele werden später in diesem Abschnitt aufgeführt.
- Melden Sie sich bei dem AWS-Konto Ort an, an dem Sie Ihre Account Factory Factory-Blueprints speichern (manchmal auch Hub-Konto genannt).
- 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 entwickelt oder heruntergeladen haben, um sie als Blueprint zu verwenden, oder fügen Sie sie ein.
- Wählen Sie unten auf der Konsolenseite die Option Produkt erstellen aus.

Sie können eine AWS CloudFormation Vorlage aus dem AWS Service Catalog Referenzarchitektur-Repository herunterladen. Ein Beispiel aus diesem Repository hilft bei der Einrichtung eines Backup-Plans für Ihre Ressourcen.

Hier ist eine Beispielvorlage für ein fiktives Unternehmen namens Best Pets. Es hilft dabei, eine Verbindung zu ihrer Haustier-Datenbank herzustellen.

```
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: nodejs16.x
      Handler: index.handler
      Timeout: 5
      Code:
        ZipFile: >
          const response = require("cfn-response");
```

```
          exports.handler = function (event, context) {
            const awsAccountId = context.invokedFunctionArn.split(":")[4]
            const connectionString= "fake connection string that's specific to account
" + awsAccountId;
            const responseData = {
              Value: connectionString,
            }
            response.send(event, context, response.SUCCESS, responseData);
            return connectionString;
          };

  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. Überprüfen Sie Ihren benutzerdefinierten Entwurf

Sie können Ihren Blueprint in der AWS Service Catalog Konsole anzeigen. Weitere Informationen finden Sie unter Produkte verwalten im Service Catalog Administrator 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 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.

> **Note**
>
> Sie müssen Ihr Customization Hub-Konto einrichten und mindestens einen Blueprint (Service Catalog-Produkt) hinzufügen, bevor Sie diese Informationen in die AWS Control Tower

Tower-Konsole eingeben und mit der Bereitstellung benutzerdefinierter Konten beginnen können.

Erstellen oder aktualisieren Sie ein benutzerdefiniertes Konto in der AWS Control Tower 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 Vorgangs 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 AWS CloudFormation Stack-Sets bereitstellen kann. Der Name der Rolle lautet `AWSControlTower-BlueprintExecution-bp-xxxx`. Die `AdministratorAccess` Richtlinie wird hier standardmäßig angewendet.
5. Wählen Sie auf der Grundlage dieses Blueprints die Regionen AWS-Region oder Regionen aus, in denen Sie Konten bereitstellen möchten.
6. Wenn Ihr Blueprint Parameter enthält, können Sie die Werte für die Parameter in zusätzliche Felder im AWS Control Tower 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 Prozess zur Kontoaktualisierung 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.

Gehen Sie wie folgt vor, um einen benutzerdefinierten Blueprint bereitzustellen, wenn Sie ein neues AWS Konto erstellen:

1. Gehen Sie zu AWS Control Tower in der AWS Management Console.
2. Wählen Sie Account Factory und 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 Organisationseinheit aus, der Ihr Konto hinzugefügt werden soll.
6. Erweitern Sie den Abschnitt „Werkseitige Anpassung des Kontos“.
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 Servicekatalog-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, sodass Sie sie ausfüllen können. Standardwerte sind vorausgefüllt.
10. Wählen Sie abschließend aus, wo Sie Ihren Blueprint bereitstellen möchten, entweder die 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 EC2-Instances oder Amazon S3 S3-Buckets, könnten in allen kontrollierten Regionen bereitgestellt werden
11. Wenn alle Felder ausgefüllt sind, wählen Sie Konto erstellen aus.

> **Note**
>
> Mit Terraform erstellte Blueprints können nur in einer Region und nicht in mehreren Regionen bereitgestellt werden.

Sie können den Fortschritt der Kontobereitstellung auf der Seite Organisation einsehen. Wenn die Bereitstellung Ihres Kontos abgeschlossen ist, sind die in Ihrem Blueprint angegebenen Ressourcen bereits darin bereitgestellt. Um die Details des Kontos und des Blueprints einzusehen, gehen Sie zur Seite mit den Kontodetails.

Registrieren Sie Konten und passen Sie sie an

Um Konten in der AWS Control Tower Tower-Konsole zu registrieren und anzupassen.

1. Navigieren Sie zur AWS Control Tower Tower-Konsole und wählen Sie in der linken Navigationsleiste Organisation aus.
2. Sie sehen eine Liste Ihrer verfügbaren Konten. Identifizieren Sie das Konto, das Sie registrieren möchten, anhand eines benutzerdefinierten Entwurfs. In der Spalte „Bundesstaat“ für dieses Konto sollte angezeigt werden, dass sich das Konto mit dem Status Nicht registriert befindet.
3. Wählen Sie das Optionsfeld links neben dem Konto und dann oben rechts auf dem Bildschirm das Drop-down-Menü Aktionen aus. 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 Organisationseinheit aus, in der Ihr Konto Mitglied werden soll.
6. Füllen Sie den Abschnitt „Werkseitige Anpassung des Kontos“ aus. Gehen Sie dabei genauso vor wie in den Abschnitten 7-12 des Verfahrens Konto erstellen. Weitere Informationen finden Sie unter Bereitstellen von Account Factory Factory-Konten mit AWS Service Catalog.

Sie können den Status Ihres Kontos auf der Seite Organisation einsehen. Wenn Ihre Kontoregistrierung abgeschlossen ist, sind die im Blueprint angegebenen Ressourcen bereits darin bereitgestellt.

Einen Blueprint zu einem AWS Control Tower Tower-Konto hinzufügen

Um einem bestehenden AWS Control Tower Tower-Mitgliedskonto einen Blueprint hinzuzufügen, folgen Sie dem Workflow Konto aktualisieren in der AWS Control Tower Tower-Konsole und wählen Sie einen neuen Blueprint aus, der dem Konto hinzugefügt werden soll. Weitere Informationen finden Sie unter Account Factory Factory-Konten mit AWS Control Tower aktualisieren und verschieben oder mit AWS Service Catalog.

> **Note**
>
> Wenn Sie einem Konto einen neuen Blueprint hinzufügen, wird der vorhandene Blueprint überschrieben.

> **Note**
>
> Pro AWS Control Tower Tower-Konto kann ein Blueprint 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 AWS 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 Tower-Konsole zur Seite Organisation.
2. Filtern Sie die Seite „Organisation“ 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 `AVAILABLE` Status befindet. Wenn sich Ihr bereitgestelltes Produkt in einem bestimmten `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 zu ändern. `AVAILABLE` Weitere Informationen finden Sie unter Bereitgestellte Produkte aktualisieren.
2. Folgen Sie dann dem Vorgang zur Kontoaktualisierung von AWS Control Tower aus, 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 zur Aktualisierung eines Blueprints, bei der der ursprüngliche Blueprint entfernt und ersetzt wird, insbesondere dann, wenn Sie Produktionsworkloads ausführen.

Entfernen Sie einen Blueprint aus einem Konto

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 Tower-Standardkonfigurationen zurückzusetzen.

Wenn Sie den Workflow „Konto aktualisieren“ in der Konsole aufrufen, werden Sie feststellen, dass alle Kontodetails ausgefüllt sind und die Anpassungsdetails nicht. Wenn Sie diese AFC-Details leer lassen, entfernt AWS Control Tower den Blueprint aus dem Konto. Bevor die Aktion beginnt, wird Ihnen 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.

Blueprints 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 für bestimmte Anwendungsfälle anzupassen. Die Blueprints der einzelnen Partner helfen Ihnen dabei, maßgeschneiderte Konten zu erstellen, die so vorkonfiguriert sind, dass sie mit den Produktangeboten dieses jeweiligen Partners funktionieren.

Eine vollständige Liste der AWS Control Tower Tower-Partner-Blueprints finden Sie in Ihrer Konsole zur Service Catalog Getting Started Library. Suchen Sie nach dem Quelltyp AWS Control Tower Blueprints.

Überlegungen zu Account Factory 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 von AWS Control Tower verwaltet werden. Eine Auswahl von 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 Tower-Verwaltungskonto. 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 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 Behelfslösungen **`AWSControlTowerBlueprintAccess`**

Wenn Sie die `AWSControlTowerBlueprintAccess` Rolle von einem AWS Control Tower Tower-Konto aus erstellen, müssen Sie mit der `AWSControlTowerExecution` Rolle als Principal angemeldet sein. Wenn Sie wie ein anderer 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) Nehmen Sie die `AWSControlTowerExecution` Rolle an und erstellen Sie die `AWSControlTowerBlueprintAccess` Rolle. Wenn Sie sich für diese Problemumgehung entscheiden, müssen Sie sich unmittelbar danach von der `AWSControlTowerExecution` Rolle abmelden, um unbeabsichtigte Änderungen an Ressourcen zu verhindern.
- Melden Sie sich bei 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 Tower-Managementkonto als Ihr Hub-Konto, sodass es nicht dem SCP unterliegt.

Anpassen Ihres Richtliniendokuments für AFC-Blueprints auf der Grundlage von CloudFormation

Wenn Sie einen Blueprint über Account Factory aktivieren, weist AWS Control Tower an, in StackSet Ihrem Namen einen AWS CloudFormation zu erstellen. AWS CloudFormation benötigt Zugriff auf Ihr verwaltetes Konto, um AWS CloudFormation Stacks in der zu erstellen. StackSet Sie verfügt über diese `AWSControlTowerExecution` Rolle zwar AWS CloudFormation bereits über Administratorrechte für das verwaltete Konto, diese Rolle kann jedoch nicht von übernommen werden. AWS CloudFormation

Im Rahmen der Aktivierung eines Blueprints erstellt AWS Control Tower eine Rolle im Mitgliedskonto, die die Ausführung der StackSet Verwaltungsaufgaben übernehmen AWS CloudFormation kann. Die einfachste Möglichkeit, Ihren benutzerdefinierten Blueprint über Account Factory zu aktivieren, ist die Verwendung einer Alles-Lass-Richtlinie, da diese Richtlinien mit jeder Blueprint-Vorlage kompatibel sind.

Bewährte Methoden empfehlen jedoch, dass Sie die Berechtigungen für AWS CloudFormation das Zielkonto einschränken müssen. Sie können eine benutzerdefinierte Richtlinie angeben, die AWS Control Tower auf die Rolle anwendet, die es für AWS CloudFormation die Verwendung erstellt hat. Wenn Ihr Blueprint beispielsweise einen SSM-Parameter mit der Bezeichnung something-important erstellt, könnten Sie die folgende Richtlinie angeben:

```
{
    "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 AWS CloudFormation verwendet diese Rolle, um Stack-Instances zu erstellen, weshalb für die Ausführung von Aktionen auf Stacks eine Genehmigung erforderlich ist. AWS CloudFormation Der `AllowSsmParameterActions` Abschnitt bezieht sich speziell auf die Vorlage, die aktiviert wird.

Probleme mit Berechtigungen lösen

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 lösen, 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 AWS CloudFormation Berechtigungen erteilt wurden und dass Sie mithilfe dieser Rolle direkt einen Stack erstellen können.

Zusätzliche Berechtigungen sind für die Erstellung eines Terraform-basierten Service Catalog-Produkts 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 bestimmte Berechtigungen hinzugefügt werden, zusätzlich zu den Berechtigungen, die zum Erstellen der in Ihrer Vorlage definierten Ressourcen erforderlich sind. Wenn Sie die standardmäßige vollständige Administratorrichtlinie wählen, müssen Sie diese zusätzlichen Berechtigungen nicht hinzufügen.

```
{
    "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 in AWS Service Catalog finden Sie unter Schritt 5: Startrollen erstellen im Service Catalog Administrator Guide.

Bereitstellen von Konten mit AWS Control Tower Account Factory for 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.

> **Note**
>
> AFT hat keinen Einfluss auf die Workflow-Leistung in AWS Control Tower. Wenn Sie ein Konto über AFT oder Account Factory bereitstellen, findet derselbe Backend-Workflow statt.

Mit AFT erstellen Sie eine Terraform-Datei für Kontoanfragen, die die Eingabe enthält, mit der der AFT-Workflow aufgerufen wird. Nach Abschluss der Kontobereitstellung und -aktualisierung wird der AFT-Workflow fortgesetzt, indem das AFT-Framework für die Kontobereitstellung und die Schritte zur Kontoanpassung ausgeführt werden.

Voraussetzungen

Bevor Sie mit AFT beginnen, müssen Sie Folgendes erstellen:

- Eine vollständig bereitgestellte AFT-Umgebung. Weitere Informationen finden Sie unter Überblick über AWS Control Tower Account Factory for Terraform (AFT) und Bereitstellen von AWS Control Tower Account Factory for Terraform (AFT)
- Ein oder mehrere `git` AFT-Repositorys in Ihrer vollständig bereitgestellten AFT-Umgebung. Weitere Informationen finden Sie unter Schritte nach der Bereitstellung von AFT.

> **Tip**
>
> Optional können Sie im aft-account-customizationsRepository einen Ordner mit Kontovorlagen erstellen.

Informationen darüber AWS-Regionen , wo AFT Einsatzbeschränkungen hat, finden Sie unter Einschränkungen und Kontingente in AWS Control Tower undEinschränkungen der Kontrolle.

Richten Sie ein neues Konto bei AFT ein

Um ein neues Konto bei AFT bereitzustellen, erstellen Sie eine Terraform-Datei mit Kontoanforderung. Diese Datei enthält die Eingabe für Parameter im aft-account-requestRepository. Nachdem Sie eine Terraform-Datei für eine Kontoanforderung 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 zur Bereitstellung von AFT-Konten.

Terraform-Dateiparameter für Kontoanfragen

Sie müssen die folgenden Parameter in Ihre Terraform-Datei für die Kontoanforderung aufnehmen. Sie können sich ein Beispiel für eine Terraform-Datei mit einer Kontoanforderung unter GitHub ansehen.

- Der Wert von `module name` muss pro Anfrage eindeutig sein. AWS-Konto
- Der Wert von `module source` ist der Pfad zum Terraform-Modul für die Kontoanforderung, das AFT bereitstellt.
- Der Wert von `control_tower_parameters` erfasst die erforderlichen Eingaben zur Erstellung eines AWS Control Tower Tower-Kontos. 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-requestRepository gehören `OUName` und`OUName (OU-ID)`.

- `account_tags`erfasst benutzerdefinierte Schlüssel und Werte, die anhand von Geschäftskriterien AWS-Konten markiert werden können. Weitere Informationen finden Sie im AWS Organizations Benutzerhandbuch unter AWS Organizations Ressourcen taggen.
- 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 angegebenen Konto unter /aft/account-request/custom-fields/ bereitgestellt werden. Sie können bei Kontoanpassungen auf diese Metadaten verweisen, um die richtigen Kontrollen einzurichten. Beispielsweise kann für ein Konto, das der Einhaltung gesetzlicher Vorschriften unterliegt, zusätzliche Funktionen bereitgestellt werden AWS-Config-Regeln. Die Metadaten, mit denen Sie Daten erfassen, `custom_fields` können bei der Kontobereitstellung und -aktualisierung zu zusätzlicher Verarbeitung führen. Wenn ein benutzerdefiniertes Feld aus der Kontoanfrage entfernt wird, wird das benutzerdefinierte Feld aus dem SSM-Parameterspeicher für das verkaufte Konto entfernt.
- (Optional) `account_customizations_name` erfasst den Kontovorlagenordner im aft-account-customizationsRepository. Weitere Informationen finden Sie unter Kontoanpassungen.

Reichen Sie mehrere Kontoanfragen ein

AFT verarbeitet Kontoanfragen nacheinander, Sie können jedoch mehrere Kontoanfragen an die AFT-Pipeline senden. Wenn Sie mehrere Kontoanfragen an die AFT-Pipeline senden, stellt AFT die Kontoanfragen in der Reihenfolge „first in, first out“ in die Warteschlange und verarbeitet sie.

> **Note**
>
> Sie können für jedes Konto, das AFT bereitstellen soll, eine Terraform-Datei für Kontoanfragen erstellen oder mehrere Kontoanfragen in einer einzigen Terraform-Datei für Kontoanfragen zusammenfassen.

Aktualisieren Sie ein bestehendes Konto

Sie können von AFT bereitgestellte Konten 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`ManagedOrganizationalUnit`, die Teil des erforderlichen Werts für ist`control_tower_parameters`, und andere Parameter in der Terraform-Datei für die Kontoanforderung aktualisieren. Weitere Informationen finden Sie unter Bereitstellen eines neuen Kontos bei AFT.

> **Note**
>
> Die Eingabe, die Sie angeben, `control_tower_parameters` kann bei der Kontobereitstellung nicht geändert werden.
> Zu den unterstützten Formaten für die Angabe `ManagedOrganizationalUnit` im aft-account-requestRepository gehören `OUName` und`OUName (OU-ID)`.

Aktualisieren Sie ein Konto, das AFT nicht bereitstellt

Sie können außerhalb von AFT erstellte AWS Control Tower Tower-Konten aktualisieren, indem Sie das Konto im aft-account-requestRepository angeben.

> **Note**
>
> Stellen Sie sicher, dass alle Kontoinformationen korrekt sind und mit der AWS Control Tower Tower-Organisation und dem jeweiligen AWS Service Catalog bereitgestellten Produkt übereinstimmen.

Voraussetzungen für die Aktualisierung eines vorhandenen Produkts AWS-Konto mit AFT

- Der AWS-Konto muss bei AWS Control Tower registriert sein.
- Sie AWS-Konto müssen Teil der AWS Control Tower Tower-Organisation sein.

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 Folgendes verfügen:

- Eine landing zone im AWS Control Tower. Weitere Informationen finden Sie unter Planen Ihrer AWS Control Tower Tower-Landezone.
- Eine Heimatregion für Ihre AWS Control Tower Tower-Landezone. Weitere Informationen finden Sie unter So AWS-Regionen arbeiten Sie mit AWS Control Tower.
- 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 einen anderen VCS-Anbieter wählen möchten, finden Sie weitere Informationen 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

Führen Sie die Schritte unter Erste Schritte mit AWS Control Tower aus. 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 (empfohlen)

Wir empfehlen, dass Sie in Ihrer AWS Organisation eine separate Organisationseinheit erstellen. Hier stellen Sie das AFT-Verwaltungskonto bereit. Erstellen Sie die neue Organisationseinheit mit Ihrem AWS Control Tower Tower-Verwaltungskonto. 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. Das AWS Control Tower Tower-Verwaltungskonto, das Ihrer AWS Control Tower Tower-Landezone zugeordnet ist, verkauft das AFT-Verwaltungskonto. 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 `1.2.0` oder höher.

Schritt 5: 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 anzeigen. 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.

Das AFT-Modul enthält einen `aft_enable_vpc` Parameter, der angibt, ob AWS Control Tower Kontoressourcen innerhalb einer Virtual Private Cloud (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.

> **Note**
>
> Wenn Sie den `aft_enable_vpc` Parameter erneut aktivieren (den Wert von `false` auf ändern`true`), müssen Sie den `terraform apply` Befehl möglicherweise zweimal hintereinander ausführen.

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 6: 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.

Schritte nach der Bereitstellung

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: (Optional) Schließen Sie den Vorgang CodeConnections mit Ihrem gewünschten VCS-Anbieter ab

Wenn Sie sich für einen VCS-Drittanbieter entscheiden 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: (Obligatorisch) 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 unterRichten Sie ein neues Konto bei AFT ein.
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 Ihres Zustandsautomaten für die AFT-Kontobereitstellungsanpassung
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 unterAnwenden globaler Anpassungen.
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 unterAnwenden von Kontoanpassungen.

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.

Überblick über AWS Control Tower Account Factory für Terraform (AFT)

Account Factory for Terraform (AFT) richtet eine Terraform-Pipeline ein, um Sie bei der Bereitstellung und Anpassung von Konten in AWS Control Tower zu unterstützen. AFT bietet Ihnen den Vorteil

der Terraform-basierten Kontobereitstellung und ermöglicht Ihnen gleichzeitig, Ihre Konten mit AWS Control Tower zu verwalten.

Mit AFT erstellen Sie eine Terraform-Datei für Kontoanfragen, 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 Pipeline zur AFT-Kontobereitstellung.

AFT unterstützt Terraform Cloud, Terraform Enterprise und Terraform Community Edition. Mit AFT können Sie die Kontoerstellung mithilfe einer Eingabedatei und eines einfachen `git push` Befehls initiieren und neue oder bestehende Konten anpassen. Die Kontoerstellung umfasst alle Vorteile von AWS Control Tower Governance und Kontoanpassungen, mit denen Sie die standardmäßigen Sicherheitsverfahren und Compliance-Richtlinien Ihres Unternehmens einhalten können.

AFT unterstützt die Rückverfolgung von Anfragen zur Kontoanpassung. Jedes Mal, wenn Sie eine Anfrage zur Kontoanpassung einreichen, generiert AFT ein eindeutiges Ablaufverfolgungstoken, das eine AWS Step Functions Zustandsmaschine für AFT-Anpassungen 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 AWS Step Functions Developer Guide

AFT kombiniert zum Aufbau eines Frameworks die Funktionen anderer AWS Dienste mit Pipelines, die Terraform Infrastructure as Code (IaC) bereitstellen. Komponentenservices AFT ermöglicht Ihnen:

- Anfragen zur Kontobereitstellung und Aktualisierung in einem GitOps Modell einreichen
- Speichern Sie Kontometadaten 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 als AFT-Verwaltungskonto bezeichnet wird, um AFT-Funktionen bereitzustellen. Bevor Sie AFT einrichten können, müssen Sie über eine bestehende AWS Control Tower Tower-Landezone verfügen. Das AFT-Verwaltungskonto ist nicht dasselbe wie das AWS Control Tower 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 stützt sich nativ auf alternative Quellen für AWS CodeCommit, unterstützt diese jedoch. CodeConnections

AFT bietet Funktionsoptionen

Sie können verschiedene Funktionsoptionen aktivieren, die auf bewährten Methoden basieren:

- Einrichtung einer Organisationsebene CloudTrail für die Protokollierung von Datenereignissen
- Löschen der AWS Standard-VPC für Konten
- Bereitgestellte Konten für den AWS Enterprise Support-Plan registrieren

> **Note**
>
> Die AFT-Pipeline ist nicht für die Bereitstellung von Ressourcen wie Amazon EC2 EC2-Instances vorgesehen, die Ihre Konten für die Ausführung Ihrer Anwendungen benötigen. Es ist ausschließlich für die automatisierte Bereitstellung und Anpassung von AWS Control Tower Tower-Konten vorgesehen.

Video-Anleitung

In diesem Video (7:33) wird beschrieben, wie Konten mit AWS Control Tower Account Factory for 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.

Videoanleitung zur automatisierten Kontobereitstellung in AWS Control Tower.

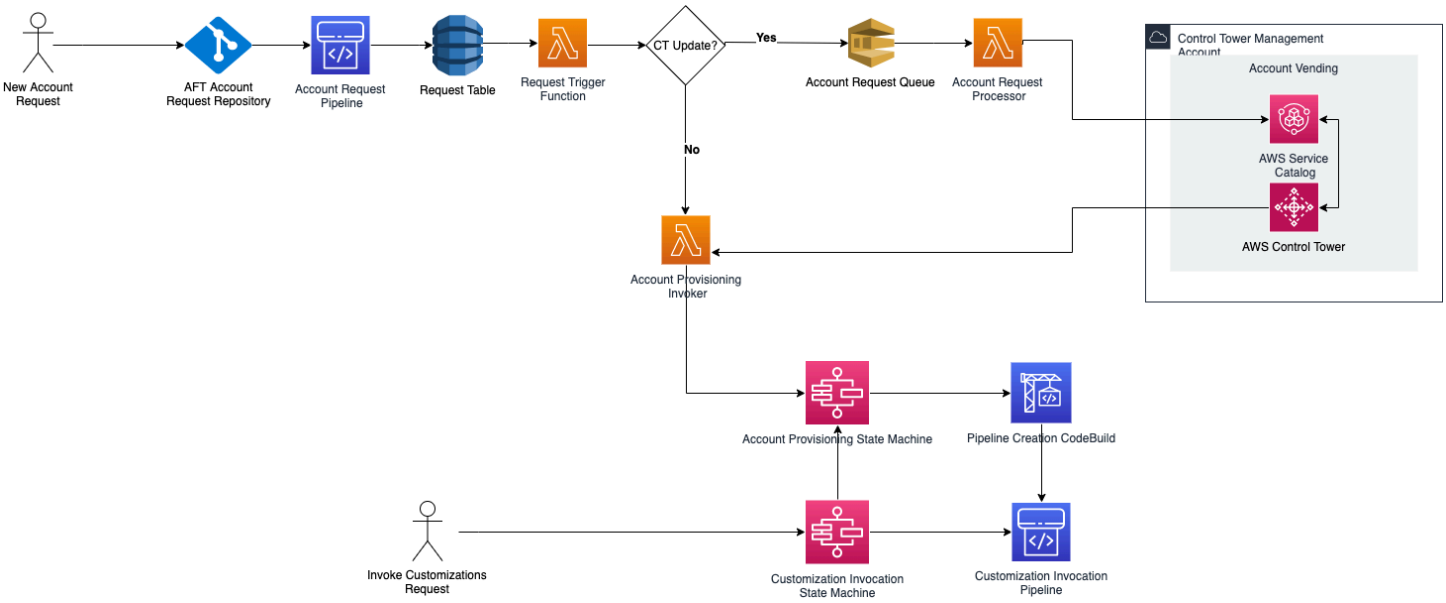
AFT-Architektur

Reihenfolge der Operationen

Sie führen AFT-Operationen im AFT-Verwaltungskonto aus. Für einen vollständigen Workflow zur Kontobereitstellung sieht die Reihenfolge der Phasen von links nach rechts im Diagramm wie folgt aus:

1. Kontoanfragen werden erstellt und an die Pipeline weitergeleitet. Sie können mehr als eine Kontoanfrage gleichzeitig erstellen und einreichen. Account Factory verarbeitet Anfragen in einer first-in-first-out Bestellung. Weitere Informationen finden Sie unter Mehrere Kontoanfragen einreichen.
2. Jedes Konto wird bereitgestellt. Diese Phase wird im AWS Control Tower Tower-Managementkonto ausgeführt.
3. Globale Anpassungen werden in den Pipelines ausgeführt, die für jedes verkaufte Konto erstellt werden.
4. Wenn Anpassungen in den ersten Anfragen zur Kontobereitstellung angegeben wurden, werden die Anpassungen nur für Zielkonten ausgeführt. Wenn Sie über ein Konto verfügen, 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



Kosten

Für AFT fallen keine zusätzlichen Gebühren an. Sie zahlen nur für die von AFT bereitgestellten Ressourcen, die von AFT bereitgestellten AWS Dienste und die Ressourcen, die Sie in Ihrer AFT-Umgebung bereitstellen.

Die AFT-Standardkonfiguration umfasst die Zuweisung von AWS PrivateLink Endpunkten für verbesserten Datenschutz und Sicherheit sowie ein NAT-Gateway, das für die Unterstützung AWS CodeBuild erforderlich ist. Einzelheiten zu den Preisen dieser Infrastruktur finden Sie in den AWS PrivateLink Preisen und den Amazon VPC-Preisen für das NAT Gateway. Für genauere Informationen zur Verwaltung dieser Kosten wenden Sie sich an Ihren AWS Kundenbetreuer. Sie können diese Standardeinstellungen für AFT ändern.

Terraform- und AFT-Versionen

Account Factory for Terraform (AFT) unterstützt die Terraform-Version oder höher. `1.2.0` Sie müssen eine Terraform-Version als Eingabeparameter für den AFT-Bereitstellungsprozess angeben, wie im folgenden Beispiel gezeigt.

```
terraform_version = "1.2.0"
```

Terraform-Verteilungen

AFT unterstützt drei Terraform-Verteilungen:

- Terraform Community Edition
- Terraform-Wolke
- 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 Distributionen Terraform Cloud oder Terraform Enterprise 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 Terraform Cloud:
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"
```

Terraform Cloud

Wenn Sie Terraform Cloud als Distribution auswählen, erstellt AFT Workspaces für die folgenden Komponenten in Ihrer Terraform Cloud-Organisation, wodurch ein API-gesteuerter Workflow initiiert wird.

- Kontoanfrage
- AFT-Anpassungen für Konten, die von AFT bereitgestellt werden
- Kontoanpassungen für Konten, die AFT bereitstellt
- Globale Anpassungen für Konten, die von AFT bereitgestellt werden

Terraform Cloud verwaltet die resultierende Terraform-State-Konfiguration.

Wenn Sie Terraform Cloud als Distribution auswählen, geben Sie die folgenden Eingabeparameter an:

- `terraform_distribution = "tfc"`
- `terraform_token`— Dieser Parameter enthält den Wert des Terraform Cloud-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 Terraform Cloud-Organisation.

> **Note**
>
> Mehrere AFT-Bereitstellungen in einer einzigen Terraform Cloud-Organisation werden nicht unterstützt.

Informationen zur Einrichtung von Terraform Cloud 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 einen API-gesteuerten 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

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.

Aktivieren von Feature-Optionen

AFT bietet Feature-Optionen, die auf bewährten Methoden basieren. Sie können sich bei der AFT-Bereitstellung mithilfe von Feature-Flags für diese Funktionen anmelden. Weitere Informationen zu AFT-Richten Sie ein neues Konto bei AFT einEingabekonfigurationsparametern finden Sie unter .

Diese Funktionen sind standardmäßig nicht aktiviert. Sie müssen jedes in Ihrer Umgebung explizit aktivieren.

Themen

- AWS CloudTrail Datenereignisse
- AWS Enterprise Support-Plan
- Löschen der AWS Standard-VPC

AWS CloudTrail Datenereignisse

Wenn diese Option aktiviert ist, konfiguriert die AWS CloudTrail Option Datenereignisse diese Funktionen.

- Erstellt einen Organisations-Trail im AWS Control Tower-Verwaltungskonto 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 Protokolldateivalidierung

Um diese Option zu aktivieren, setzen Sie das folgende Feature-Flag in Ihrer AFT-Bereitstellungseingabekonfiguration auf True.

```
aft_feature_cloudtrail_data_events
```

Voraussetzung

Bevor Sie diese Feature-Option 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 Services > CloudTrail aus.
3. Wählen Sie dann bei Bedarf oben rechts Vertrauenswürdigen Zugriff aktivieren aus.

Möglicherweise erhalten Sie eine Warnmeldung, in der Sie zur Verwendung der AWS CloudTrail Konsole aufgefordert werden, aber in diesem Fall ignorieren Sie die Warnung. AFT erstellt den Trail als Teil der Aktivierung dieser Feature-Option, 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 sind zum Zeitpunkt der Aktivierung von Amazon S3-Datenereignissen ausgeschlossen. Weitere Informationen zu finden Sie im AWS CloudTrail -Benutzerhandbuch CloudTrail.

AWS Enterprise Support-Plan

Wenn diese Option aktiviert ist, aktiviert die AFT-Pipeline den AWS Enterprise Support-Plan für Konten, die von AFT bereitgestellt werden.

AWS Für -Konten ist standardmäßig der AWS Basic Support-Plan aktiviert. AFT bietet eine automatisierte Registrierung für den Unternehmenssupport für Konten, die von AFT bereitgestellt

werden. Der Bereitstellungsprozess öffnet ein Support-Ticket für das Konto und fordert auf, es dem AWS Enterprise-Support-Plan hinzuzufügen.

Um die Option Enterprise Support zu aktivieren, setzen Sie das folgende Feature-Flag in Ihrer AFT-Bereitstellungseingabekonfiguration auf True.

```
aft_feature_enterprise_support=false
```

Weitere Informationen zu AWS Support-Plänen finden Sie unter Vergleichen von AWS Support-Plänen.

> **Note**
>
> Damit diese Funktion ausgeführt werden kann, müssen Sie das Zahlerkonto im Enterprise Support-Plan registrieren.

Löschen der AWS Standard-VPC

Wenn Sie diese Option aktivieren, löscht AFT alle AWS Standard-VPCs im Verwaltungskonto und in allen AWS-Regionen, auch wenn keine AWS Control Tower-Ressourcen in diesen bereitgestellt haben AWS-Regionen.

AFT löscht AWS Standard-VPCs nicht automatisch für AWS Control Tower-Konten, die von AFT bereitgestellt werden, oder für bestehende AWS Konten, die Sie über AFT bei AWS Control Tower registrieren.

Neue AWS Konten werden standardmäßig mit einer VPC erstellt AWS-Region, die in jeder eingerichtet ist. Ihr Unternehmen verfügt möglicherweise über Standardmethoden für die Erstellung von VPCs, bei denen Sie die AWS Standard-VPC löschen und die Aktivierung vermeiden müssen, insbesondere für das AFT-Verwaltungskonto.

Um diese Option zu aktivieren, setzen Sie das folgende Feature-Flag in Ihrer AFT-Bereitstellungseingabekonfiguration auf True.

```
aft_feature_delete_default_vpcs_enabled
```

Weitere Informationen zu Standard-VPCs finden Sie unter Standard-VPC und Standard-SubnetzeVPCs.

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.

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	AWSAFTAdministrator AWSAFTExecution AWSAFTService aws-ct-aft-*
AWS Identity and Access Management	Richtlinien	aws-ct-aft-*
CodeCommit	Repositorys	aws-ct-aft-*
CodeBuild	Build-Projekte	aws-ct-aft-*
Code-Pipeline	Pipelines	*-baseline-*
Amazon S3	Buckets	*-aws-ct-aft-*

AWS Service nicht zulässig	Ressourcentyp	Ressourcenname
		aws-ct-aft-*
Lambda	Funktionen	aws-ct-aft-*
Lambda	Ebenen	aws-ct-aft-common-layer
DynamoDB	Tabellen	aws-ct-aft-request aws-ct-aft-request-audit aws-ct-aft-request-metadata aws-ct-aft-controltower-events
Step Functions	Staatsmaschinen	aws-ct-aft-prebaseline aws-ct-aft-prebaseline-customizations aws-ct-aft-trigger-baseline aws-ct-aft-features
VPC	VPC	aws-ct-aft-vpc
Amazon SNS	Themen	aws-ct-aft-notifications aws-ct-aft-failure-notifications
Amazon EventBridge	Ereignisbusse	aws-ct-aft-events-from-ct-management
Amazon EventBridge	Regeln für Veranstaltungen	aws-ct-aft-capture-ct-events aws-ct-aft-lambda-account-request-processor
Schlüsselverwaltungsdienst (KMS)	Vom Kunden verwaltete Schlüssel	*-aws-ct-aft-* aws-ct-aft-*

AWS Service nicht zulässig	Ressourcentyp	Ressourcenname
AWS Systems Manager	Parameter speichern	/aws-ct-aft/account/* /aws/ct-aft/config/*
Amazon SQS	Warteschlangen	aws-ct-aft-account-request.fifo aws-ct-aft-account-request-dlg.fifo
CloudWatch	Protokollgruppen	/aws/*/aws-ct-aft-* aws-ct-aft-*
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	AWSAFTExecutionRole AWSAFTExecution aws-ct-aft-controltower-events-rule

AWS Service nicht zulässig	Ressourcentyp	Ressourcenname
AWS Systems Manager	Parameter speichern	/aws-ct-aft/account/aws-ct-aft-management/account-id
AWS Organizations (Fakultativ)	Service-Kontrollrichtlinien	aws-ct-aft-protect-resources
CloudTrail (Fakultativ)	Trails	aws-ct-aft-BaselineCloudTrail
AWS-Supportcenter (optional)	Unterstützungspläne	Enterprise

AWS Control Tower Tower-Protokollarchiv-Konto

AWS Service nicht zulässig	Ressourcentyp	Ressourcenname
AWS Identity and Access Management	Rollen	AWSAFTExecutionRole AWSAFTExecution aws-ct-aft-cloudtrail-data-events-role
Schlüsselverwaltungsservice (KMS)	Vom Kunden verwaltete Schlüssel	*-aws-ct-aft-kms-gd-findings
Amazon S3	Buckets	*-aws-ct-aft-logs* aws-ct-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	AWSAFTExecutionRole

AWS Service nicht zulässig	Ressourcentyp	Ressourcenname
		AWSAFTExecution
AWS Kundendienstzentrum (optional)	Unterstützungspläne	Enterprise

Erforderliche Rollen

Im Allgemeinen sind Rollen und Richtlinien Teil von Identity and Access Management (IAM) in AWS. Weitere Informationen finden Sie im AWS IAM-Benutzerhandbuch.

AFT erstellt mehrere IAM-Rollen und -Richtlinien in den Verwaltungskonten AFT Management und AWS Control Tower, um den Betrieb der AFT-Pipeline zu unterstützen. Diese Rollen werden auf der Grundlage des Zugriffsmodells mit den geringsten Berechtigungen erstellt, das die Berechtigung auf die minimal erforderlichen Aktionen und Ressourcen für jede Rolle und Richtlinie beschränkt. Diesen Rollen und Richtlinien wird ein - AWS Tag-`key:value`Paar zugewiesen, das `managed_by:AFT` zur Identifizierung bestimmt ist.

Neben diesen IAM-Rollen erstellt AFT drei wesentliche Rollen:

- die `AWSAFTAdmin` Rolle
- die `AWSAFTExecution` Rolle
- die `AWSAFTService` Rolle

Diese Rollen werden in den folgenden Abschnitten erläutert.

Die erläuterte AWSAFTAdmin Rolle

Wenn Sie AFT bereitstellen, wird die `AWSAFTAdmin` Rolle im AFT-Verwaltungskonto erstellt. Diese Rolle ermöglicht es der AFT-Pipeline, die `AWSAFTExecution` Rolle in AWS Control Tower und von AFT bereitgestellten Konten zu übernehmen und so Aktionen im Zusammenhang mit der Bereitstellung und Anpassung von Konten durchzuführen.

Hier ist die Inline-Richtlinie (JSON-Artefakt), die der `AWSAFTAdmin` Rolle zugeordnet ist:

```
{
    "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 Vertrauensstellung für die `AWSAFTAdmin` Rolle. Die Platzhalternummer `012345678901` wird durch die ID-Nummer des AFT-Verwaltungskontos ersetzt.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::012345678901:root"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Die erläuterte AWSAFTExecution Rolle

Wenn Sie AFT bereitstellen, wird die `AWSAFTExecution` Rolle in den Verwaltungskonten AFT Management 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 zunächst die `AWSControlTowerExecution` Rolle , 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 Bereitstellungsanpassungsphasen des AFT-Frameworks, für von AFT bereitgestellte Konten und für gemeinsam genutzte Konten ausgeführt werden.

> **Verschiedene Rollen helfen Ihnen, den Umfang einzuschränken**
>
> Als bewährte Methode sollten Sie die Anpassungsberechtigungen von den Berechtigungen trennen, die während der ersten Bereitstellung von Ressourcen zulässig sind. Denken Sie daran, dass die `AWSAFTService` Rolle für die Kontobereitstellung und die `AWSAFTExecution` Rolle für die Kontoanpassung vorgesehen ist. Diese Trennung schränkt den Umfang der Berechtigungen ein, die während jeder Phase der Pipeline zulässig sind. Diese Unterscheidung ist besonders wichtig, wenn Sie die freigegebenen Konten von AWS Control Tower anpassen, da die freigegebenen Konten möglicherweise vertrauliche Informationen wie Abrechnungsdetails oder Benutzerinformationen enthalten.

Berechtigungen für Rolle`AWSAFTExecution`: AdministratorAccess – eine von AWS verwaltete Richtlinie

Das folgende JSON-Artefakt zeigt die IAM-Richtlinie (Vertrauensbeziehung), die der `AWSAFTExecution` Rolle zugeordnet ist. Die Platzhalternummer `012345678901` wird durch die ID-Nummer des AFT-Verwaltungskontos ersetzt.

Vertrauensrichtlinie für `AWSAFTExecution`

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::012345678901:role/AWSAFTAdmin"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Die erläuterte AWSAFTService Rolle

Die `AWSAFTService` Rolle stellt AFT-Ressourcen in allen registrierten und verwalteten Konten bereit, einschließlich der freigegebenen Konten und des Verwaltungskontos. Ressourcen wurden früher nur von der `AWSAFTExecution` Rolle bereitgestellt.

Die `AWSAFTService` Rolle ist für die Verwendung durch die Service-Infrastruktur zur Bereitstellung von Ressourcen während der Bereitstellungsphase vorgesehen, und die `AWSAFTExecution` Rolle ist nur für die Bereitstellung von Anpassungen vorgesehen. Indem Sie die Rollen auf diese Weise übernehmen, können Sie in jeder Phase eine detailliertere Zugriffskontrolle aufrechterhalten.

Berechtigungen für `AWSAFTService` Rolle: AdministratorAccess – eine von AWS verwaltete Richtlinie

Das folgende JSON-Artefakt zeigt die IAM-Richtlinie (Vertrauensbeziehung), die der `AWSAFTService` Rolle zugeordnet ist. Die Platzhalternummer `012345678901` wird durch die ID-Nummer des AFT-Verwaltungskontos ersetzt.

Vertrauensrichtlinie für `AWSAFTService`

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::012345678901:role/AWSAFTAdmin"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Komponentenservices

Wenn Sie AFT bereitstellen, werden Komponenten von jedem dieser AWS Services zu Ihrer AWS Umgebung 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 Kontoanforderungen, der Prüfungsverlauf von Kontoaktualisierungen, Kontometadaten und Lebenszyklusereignisse von AWS Control Tower gespeichert werden. AFT erstellt auch DynamoDB-Lambda-Auslöser, um nachgelagerte Prozesse zu initiieren, z. B. den Workflow für die 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, die Protokolle speichern, die von den AWS-Services generiert werden, die die AFT-Pipeline benötigt. AFT erstellt auch einen Terraform-Backend-S3-Bucket in primären und sekundären AWS-Regionen, um Terraform-Zustände zu speichern, die während AFT-Pipeline-Workflows generiert wurden.
- Amazon Simple Notification Service – AFT erstellt Amazon Simple Notification Service (SNS)-Themen im AFT-Verwaltungskonto, in dem Erfolgs- und Fehlerbenachrichtigungen nach der Verarbeitung jeder AFT-Kontoanforderung gespeichert werden. Möglicherweise erhalten Sie diese Nachrichten mit einem Protokoll Ihrer Wahl.
- Amazon Simple Queuing Service – AFT erstellt eine Amazon Simple Queuing Service (Amazon SQS) FIFO-Warteschlange im AFT-Verwaltungskonto. Die Warteschlange ermöglicht es Ihnen, mehrere Kontoanforderungen parallel zu senden, sendet jedoch jeweils eine Anforderung zur sequenziellen Verarbeitung an AWS Control Tower Account Factory.
- AWS CodeBuild – AFT erstellt AWS- CodeBuild Build-Projekte im AFT-Verwaltungskonto, um Terraform-Pläne für AFT-Quellcode in verschiedenen Build-Phasen zu initialisieren, zu kompilieren, zu testen und anzuwenden.
- AWS CodePipeline – AFT erstellt AWS- CodePipeline Pipelines im AFT-Verwaltungskonto, um sie in den von Ihnen ausgewählten, unterstützten AWS- CodeStar Verbindungsanbieter für AFT-Quellcode zu integrieren und Build-Aufträge in AWS auszulösen CodeBuild.
- AWS Lambda – AFT erstellt AWS Lambda-Funktionen und -Ebenen im AFT-Verwaltungskonto, um Schritte während der Kontoanforderung, AFT-Kontobereitstellung und Kontoanpassungsprozesse auszuführen.
- AWS Systems Manager Parameter Store – AFT richtet den AWS Systems Manager Parameter Store im AFT-Verwaltungskonto ein, um die für die AFT-Pipelineprozesse erforderlichen Konfigurationsparameter zu speichern.
- Amazon CloudWatch – AFT erstellt Amazon- CloudWatch Protokollgruppen im AFT-Verwaltungskonto, um Protokolle zu speichern, die von AWS-Services generiert werden, die von der AFT-Pipeline genutzt werden. Der Aufbewahrungszeitraum für CloudWatch Protokolle ist auf festgelegt`Never Expire`.
- Amazon VPC – AFT erstellt eine Amazon Virtual Private Cloud (VPC), um Services 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-Status, Daten, die in DynamoDB-Tabellen gespeichert sind, und SNS-Themen.

Diese Protokolle und Artefakte werden generiert, wenn AWS-Ressourcen und -Services von AFT bereitgestellt werden. Von AFT erstellte KMS-Schlüssel haben die jährliche Drehung standardmäßig aktiviert.

- AWS Identity and Access Management (IAM) – AFT folgt dem empfohlenen Modell mit den geringsten Rechten. Es erstellt AWS Identity and Access Management (IAM)-Rollen und -Richtlinien im AFT-Verwaltungskonto, in AWS-Control-Tower-Konten und in von AFT bereitgestellten Konten nach Bedarf, um Aktionen auszuführen, die während des AFT-Pipeline-Workflows erforderlich sind.
- AWS Step Functions – AFT erstellt AWS Step Functions-Zustandsautomaten im AFT-Verwaltungskonto. Diese Zustandsautomaten orchestrieren und automatisieren den Prozess und die Schritte für das AFT-Kontobereitstellungs-Framework und die Anpassungen.
- Amazon EventBridge – AFT erstellt einen Amazon EventBridge Event Bus im AFT- und AWS Control Tower-Verwaltungskonto, um Lebenszyklusereignisse von AWS Control Tower langfristig in der DynamoDB-Tabelle des AFT-Verwaltungskontos zu erfassen und zu speichern. AFT erstellt AWS- CloudWatch Ereignisregeln in den Verwaltungskonten AFT Management und AWS Control Tower, 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 Organisations-Trail 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 Protokollarchivkonto von AWS Control Tower.
- AWS Support (optional) – Wenn diese Funktion aktiviert ist, aktiviert AFT den AWS Enterprise Support-Plan für Konten, die von AFT bereitgestellt werden. Standardmäßig werden AWS-Konten mit aktiviertem AWS Basic Support-Plan erstellt.

Pipeline zur 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 aus, um sicherzustellen, dass die neu bereitgestellten Konten über 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 Kontoanpassungsphase durchzuführen, da diese Rolle Zugriff auf das Account-Factory-Portfolio gewährt.
5. Wendet die Konto-Tags an, die Sie als Teil der Eingabeparameter der Kontoanforderung angegeben haben.
6. Wendet die AFT-Funktionsoptionen an, die Sie zum Zeitpunkt der AFT-Bereitstellung ausgewählt haben.
7. Wendet die von Ihnen bereitgestellten Anpassungen der AFT-Kontobereitstellung an. Im nächsten Abschnitt erfahren Sie mehr darüber, wie Sie diese Anpassungen mit einem AWS Step Functions-Zustandsautomaten in einem `git`Repository einrichten. Diese Phase wird manchmal als Framework-Phase für die Kontobereitstellung bezeichnet. Es ist Teil des Kernbereitstellungsprozesses, aber Sie haben zuvor ein Framework eingerichtet, das im Rahmen Ihres Kontobereitstellungs-Workflows benutzerdefinierte Integrationen bereitstellt, bevor den Konten in der nächsten Phase zusätzliche Anpassungen hinzugefügt werden.
8. Für jedes bereitgestellte Konto wird ein AWS CodePipeline im AFT-Verwaltungskonto erstellt, das ausgeführt wird, um die (nächste, globale) Anpassungen des Kontos Phase durchzuführen.
9. Ruft die Pipeline für Kontoanpassungen für jedes bereitgestellte (und gezielte) Konto auf.
10. Sendet eine Erfolgs- oder Fehlerbenachrichtigung an das SNS-Thema, aus dem Sie die Nachrichten abrufen können.

Einrichten der Framework-Anpassungen für die Kontobereitstellung mit einem Zustandsautomaten

Wenn Sie vor der Bereitstellung Ihrer Konten benutzerdefinierte Nicht-Terraform-Integrationen einrichten, sind diese Anpassungen in Ihrem AFT-Workflow zur Kontobereitstellung enthalten. Sie können beispielsweise bestimmte Anpassungen erfordern, um sicherzustellen, dass alle von AFT erstellten Konten den Standards und Richtlinien Ihrer Organisation entsprechen, z. B. Sicherheitsstandards, und diese Standards können vor der zusätzlichen Anpassung zu Konten hinzugefügt werden. Diese Framework-Anpassungen für die Kontobereitstellung werden auf jedem bereitgestellten Konto implementiert, bevor die globale Kontoanpassungsphase als Nächstes beginnt.

> **Note**
>
> Die in diesem Abschnitt beschriebene AFT-Funktion richtet sich an fortgeschrittene Benutzer, die die Funktion von AWS Step Functions verstehen. Als Alternative empfehlen wir Ihnen, in der Phase der Kontoanpassung mit den globalen Helfern zu arbeiten.

Das AFT-Framework zur Kontobereitstellung ruft einen AWS Step Functions-Zustandsautomaten auf, den Sie definieren, um Ihre Anpassungen zu implementieren. Weitere Informationen zu den möglichen Integrationen von Zustandsautomaten finden Sie in der AWS Step Functions-Dokumentation.

Hier sind einige gängige Integrationen.

- AWS Lambda-Funktionen in der Sprache Ihrer Wahl
- AWS ECS- oder AWS Fargate-Aufgaben unter Verwendung von Docker-Containern
- AWS Step Functions-Aktivitäten mit benutzerdefinierten Workern, die entweder in AWS oder On-Premises gehostet werden
- Amazon SNS- oder SQS-Integrationen

Wenn kein AWS Step Functions -Zustandsautomatdefiniert ist, wird die Stufe ohne Betrieb bestanden. Um einen Zustandsautomaten für die AFT-Kontobereitstellungsanpassung zu erstellen, folgen Sie den Anweisungen unter Erstellen Ihres Zustandsautomaten für die AFT-Kontobereitstellungsanpassung. Bevor Sie Anpassungen hinzufügen, stellen Sie sicher, dass Sie über die Voraussetzungen verfügen.

Diese Integrationstypen sind nicht Teil von AWS Control Tower und können während der globalen Pre-API-Phase der AFT-Kontoanpassung nicht hinzugefügt werden. Stattdessen können Sie diese Anpassungen im Rahmen des Bereitstellungsprozesses mit der AFT-Pipeline einrichten und sie werden im Bereitstellungsworkflow ausgeführt. Sie müssen diese Anpassungen implementieren, indem Sie Ihren Zustandsautomaten im Voraus erstellen, bevor Sie die AFT-Kontobereitstellungsphase starten, wie in den folgenden Abschnitten beschrieben.

Voraussetzungen für das Erstellen eines Zustandsautomaten

- Eine vollständig bereitgestellte AFT. Weitere Informationen Stellen Sie AWS Control Tower Account Factory für Terraform (AFT) bereit zur AFT-Bereitstellung finden Sie unter .

- Richten Sie in Ihrer Umgebung ein `git`Repository für Anpassungen der AFT-Kontobereitstellung ein. Weitere Informationen finden Sie unter Schritte nach der Bereitstellung.

Erstellen Ihres Zustandsautomaten für die AFT-Kontobereitstellungsanpassung

Schritt 1: Ändern der Definition des Zustandsautomaten

Ändern Sie die Definition des Beispiels für einen `customizations.asl.json` Zustandsautomaten. Das Beispiel ist in dem `git`Repository verfügbar, das Sie zum Speichern von Anpassungen der AFT-Kontobereitstellung eingerichtet haben, in Ihren Schritten nach der Bereitstellung. Weitere Informationen zu Definitionen von Zustandsautomaten finden Sie im AWS Step Functions-Entwicklerhandbuch.

Schritt 2: Die entsprechende Terraform-Konfiguration einschließen

Fügen Sie Terraform-Dateien mit der `.tf` Erweiterung in dasselbe `git`Repository mit der Definition des Zustandsautomaten für Ihre benutzerdefinierte Integration ein. Wenn Sie beispielsweise eine Lambda-Funktion in Ihrer Aufgabendefinition des Zustandsautomaten aufrufen möchten, fügen Sie die `lambda.tf` Datei in dasselbe Verzeichnis ein. Stellen Sie sicher, dass Sie die erforderlichen IAM-Rollen und -Berechtigungen für Ihre benutzerdefinierten Konfigurationen angeben.

Wenn Sie die entsprechende Eingabe bereitstellen, ruft die AFT-Pipeline Ihren Zustandsautomaten automatisch auf und stellt Ihre Anpassungen im Rahmen der Framework-Phase für die Bereitstellung von AFT-Konten bereit.

So starten Sie das Framework und die Anpassungen für die AFT-Kontobereitstellung neu

AFT führt das Framework zur Kontobereitstellung aus und passt die Schritte für jedes Konto an, das über die AFT-Pipeline verkauft wird. Um Anpassungen der Kontobereitstellung neu zu starten, können Sie eine dieser beiden Methoden verwenden:

1. Nehmen Sie Änderungen an einem vorhandenen Konto im Kontoanforderungs-Repo vor.
2. Stellen Sie ein neues Konto mit AFT bereit.

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 Reihe von Konten oder in einzelnen Konten implementieren. Sie können Python-Skripte, Bash-Skripte und Terraform-Konfigurationen ausführen oder im Rahmen Ihrer Kontoanpassungsphase mit der AWS CLI interagieren.

Übersicht

Nachdem Ihre Anpassungen in den von Ihnen ausgewählten `git` Repositorys angegeben wurden, entweder in denen Sie Ihre globalen Anpassungen speichern oder in denen Sie Ihre Kontoanpassungen speichern, wird die Phase der Kontoanpassung automatisch von der AFT-Pipeline abgeschlossen. Informationen zum rückwirkenden Anpassen von Konten finden Sie unter Erneutes Aufrufen von Anpassungen.

Globale Anpassungen (optional)

Sie können bestimmte Anpassungen auf alle Konten anwenden, die von AFT bereitgestellt werden. Wenn Sie beispielsweise eine bestimmte IAM-Rolle erstellen oder in jedem Konto eine benutzerdefinierte Kontrolle bereitstellen müssen, ermöglicht Ihnen die Phase der globalen Anpassungen in der AFT-Pipeline dies automatisch.

Kontoanpassungen (optional)

Um ein einzelnes Konto oder eine Gruppe von Konten anders als andere von AFT bereitgestellte Konten anzupassen, können Sie den Teil der AFT-Pipeline zur Kontoanpassung nutzen, um kontospezifische Konfigurationen zu implementieren. Beispielsweise benötigt nur ein bestimmtes Konto möglicherweise 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.

- Eine vollständig bereitgestellte AFT. Weitere Informationen zur Bereitstellung finden Sie unter Konfigurieren und starten Sie Ihre AWS Control Tower Account Factory für Terraform.
- Vorausgefüllte `git` Repositorys für globale Anpassungen und Kontoanpassungen in Ihrer Umgebung. Weitere Informationen finden Sie unter Schritt 3: Füllen jedes Repositorys in Schritte nach der Bereitstellung .

Anwenden globaler Anpassungen

Um globale Anpassungen anzuwenden, müssen Sie eine bestimmte Ordnerstruktur in das von Ihnen gewählte Repository verschieben.

- Wenn Ihre benutzerdefinierten Konfigurationen in Form von Python-Programmen oder -Skripts vorliegen, platzieren Sie diese im Ordner api_helpers/python in Ihrem Repository.
- Wenn Ihre benutzerdefinierten Konfigurationen in Form von Bash-Skripten vorliegen, platzieren Sie diese in Ihrem Repository unter dem Ordner api_helpers.
- Wenn Ihre benutzerdefinierten Konfigurationen die Form von Terraform haben, platzieren Sie diese im Terraform-Ordner in Ihrem Repository.
- Weitere Informationen zum Erstellen von benutzerdefinierten Konfigurationen finden Sie in der README-Datei für globale Anpassungen.

> **Note**
>
> Globale Anpassungen werden nach der AFT-Kontobereitstellungs-Framework-Phase in der AFT-Pipeline automatisch angewendet.

Anwenden von Kontoanpassungen

Sie können Kontoanpassungen anwenden, indem Sie eine bestimmte Ordnerstruktur in das von Ihnen gewählte Repository verschieben. Kontoanpassungen werden automatisch in der AFT-Pipeline und nach der Phase der globalen Anpassungen angewendet. Sie können auch mehrere Ordner erstellen, die unterschiedliche Kontoanpassungen in Ihrem Repository für Kontoanpassungen enthalten. Gehen Sie für jede erforderliche Kontoanpassung wie folgt vor.

So wenden Sie Kontoanpassungen an

1. Schritt 1: Erstellen eines Ordners für eine Kontoanpassung

   Kopieren Sie in dem von Ihnen ausgewählten Repository den von AFT bereitgestellten `ACCOUNT_TEMPLATE` Ordner in einen neuen Ordner. Der Name Ihres neuen Ordners sollte mit dem übereinstimmen`account_customizations_name`, den Sie in Ihrer Kontoanforderung angeben.
2. Fügen Sie die Konfigurationen zu Ihrem spezifischen Ordner für Kontoanpassungen hinzu

Sie können Ihrem Ordner für Kontoanpassungen je nach Format Ihrer Konfigurationen Konfigurationen Konfigurationen hinzufügen.

- Wenn Ihre benutzerdefinierten Konfigurationen in Form von Python-Programmen oder -Skripts vorliegen, platzieren Sie sie unter dem Ordner ***[account_customizations_name]***/api_helpers/python, der sich in Ihrem Repository befindet.
- Wenn Ihre benutzerdefinierten Konfigurationen in Form von Bash-Skripten vorliegen, platzieren Sie sie unter dem Ordner ***[account_customizations_name]***/api_helpers, der sich in Ihrem Repository befindet.
- Wenn Ihre benutzerdefinierten Konfigurationen die Form von Terraform haben, platzieren Sie sie in den 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. Verweisen Sie auf den spezifischen **`account_customizations_name`** Parameter in der Kontoanforderungsdatei

   Die Anforderungsdatei des AFT-Kontos 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 verschiedene oder ähnliche Kontoanpassungen anwenden möchten, geben Sie die Kontoanpassungen mit dem `account_customizations_name` Eingabeparameter in Ihren Kontoanforderungen an. Weitere Informationen finden Sie unter Senden mehrerer Kontoanforderungen.

Erneutes Aufrufen von 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 event-source-based erneuter Aufruf ermöglicht es Ihnen, Anpassungen auf einzelne Konten, auf alle Konten, auf Konten entsprechend ihrer Organisationseinheit oder auf Konten anzuwenden, die gemäß Tags ausgewählt wurden.

Gehen Sie wie folgt vor, um Anpassungen für von AFT bereitgestellte Konten erneut aufzurufen.

Schritt 1: Übertragen von Änderungen an globale oder Kontoanpassungs**`git`**-Repositorys

Sie können Ihre globalen und Kontoanpassungen nach Bedarf aktualisieren und Änderungen an Ihre `git` Repositorys zurücksenden. An diesem Punkt passiert nichts, die Anpassungspipeline muss von einer Ereignisquelle aufgerufen werden, wie in den nächsten beiden Schritten erläutert.

Schritt 2: Starten einer AWS Step Function-Ausführung zum erneuten Aufrufen von Anpassungen

AFT stellt eine AWS Step Function namens `aft-invoke-customizations` im AFT-Verwaltungskonto bereit. Der Zweck dieser Funktion besteht darin, die Anpassungspipeline für von AFT bereitgestellte 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-Ereignisschema zeigt, dass Sie Konten auswählen können, die beim erneuten Aufruf berücksichtigt oder ausgeschlossen werden sollen. Sie können nach Organisationseinheit (OU), Konto-Tags und Konto-ID filtern. Wenn Sie keine Filter anwenden und die Anweisung einschließen`"type":"all"`, wird die Anpassung für alle von AFT bereitgestellten Konten erneut aufgerufen.

> **Note**
>
> Wenn Ihre Version von AWS Control Tower 1.6.5 oder höher ist, können Sie verschachtelte OUs mit der Syntax anvisieren`OU Name (ou-id-1234`.) Weitere Informationen finden Sie im folgenden Thema auf GitHub.

Nachdem Sie die Ereignisparameter ausgefüllt haben, führt Step Functions aus und ruft die entsprechenden Anpassungen auf. AFT kann maximal 5 Anpassungen gleichzeitig aufrufen. Step Functions wartet und führt Schleifen aus, bis alle Konten, die den Ereigniskriterien entsprechen, abgeschlossen sind.

Schritt 3: Überwachen Sie die AWS Step Function-Ausgabe und beobachten Sie, wie AWS CodePipeline ausgeführt wird

- Die resultierende Step-Function-Ausgabe enthält Konto-IDs, die mit der Step-Function-Eingabeereignisquelle übereinstimmen.
- Navigieren Sie zu AWS CodePipeline unter Entwicklertools und zeigen Sie die entsprechenden Anpassungspipelines für die Konto-ID an.

Fehlerbehebung mit der Nachverfolgung von Anforderungen zur Anpassung von AFT-Konten

Workflows zur Kontoanpassung, die auf AWS Lambda -Protokollen basieren, die Zielkonto- und Anpassungsanforderungs-IDs enthalten. Mit AFT können Sie Anpassungsanforderungen mit Amazon CloudWatch Logs verfolgen und Fehler beheben, indem Sie CloudWatch Logs-Insights-Abfragen bereitstellen, mit denen Sie CloudWatch Protokolle im Zusammenhang mit Ihrer Anpassungsanforderung nach Ihrem Zielkonto oder Ihrer Anpassungsanforderungs-ID filtern können. Weitere Informationen finden Sie unter Analysieren von Protokolldaten mit Amazon CloudWatch Logs im Amazon- CloudWatch Logs-Benutzerhandbuch.

So verwenden Sie CloudWatch Logs Insights für AFT

1. Öffnen Sie die - CloudWatch Konsole unter https://console.aws.amazon.com/cloudwatch/.
2. Wählen Sie im Navigationsbereich Protokolle und dann Logs Insights aus.
3. Wählen Sie Abfragen aus.
4. Wählen Sie unter Beispielabfragen die Option Account Factory für Terraform und dann eine der folgenden Abfragen aus:

   - Anpassen von Protokollen nach Konto-ID

     > **Note**
     >
     > Stellen Sie sicher, dass Sie *„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/
     ```

   - Anpassen von Protokollen nach Anpassungsanforderungs-ID

     > **Note**
     >
     > Ersetzen Sie unbedingt *„YOUR-CUSTOMIZATION-REQUEST-ID“* durch Ihre Anpassungsanforderungs-ID. Ihre Anpassungsanforderungs-ID finden Sie in

der Ausgabe des AFT-Kontobereitstellungs-Framework- AWS Step Functions Zustandsautomaten. Weitere Informationen zum AFT-Kontobereitstellungs-Framework finden Sie unter AFT-Kontobereitstellungs-Pipeline

```
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.

Alternativen zur Versionskontrolle von Quellcode in AFT

AFT verwendet standardmäßig ein Versionskontrollsystem (VCS) AWS CodeCommit für Quellcode, ermöglicht aber auch andere, CodeConnectionsdie Ihren Geschäftsanforderungen oder der vorhandenen Architektur entsprechen. Sie können im Rahmen der Voraussetzungen für die AFT-Bereitstellung ein VCS eines Drittanbieters angeben.

AFT unterstützt die folgenden Alternativen zur Quellcodeverwaltung:

- GitHub
- GitHub Unternehmensserver
- BitBucket

Wenn Sie es AWS CodeCommit als Ihren VCS auswählen, sind keine zusätzlichen Schritte erforderlich. Standardmäßig erstellt AFT 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 in Ihrer von AFT unterstützten VCS-Drittanbieter-Umgebung `git` Repositorys für die folgenden Elemente erstellen.

- AFT-Kontoanfragen. Beispielcode verfügbar. Weitere Informationen zu AFT-Kontoanfragen finden Sie unterRichten Sie ein neues Konto bei AFT ein.
- Anpassungen bei der Bereitstellung von AFT-Konten. Beispielcode verfügbar. Weitere Informationen zu Anpassungen der AFT-Kontobereitstellung finden Sie unter. Erstellen Ihres Zustandsautomaten für die AFT-Kontobereitstellungsanpassung
- 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"`, oder an.
- github_enterprise_url: Geben Sie die URL nur für Enterprise-Kunden an. GitHub GitHub
- account_request_repo_name: Standardmäßig ist dieser Wert auf für Benutzer festgelegt. `aft-account-request` AWS CodeCommit Wenn Sie Ihr Repository mit einem neuen Namen in CodeCommit oder in einer von AFT unterstützten VCS-Provider-Umgebung eines Drittanbieters erstellt haben, aktualisieren Sie diesen Eingabewert mit Ihrem tatsächlichen Repository-Namen. Für BitBucket Github und GitHub Enterprise muss der Repository-Name das folgende Format haben. `[Org]/[Repo]`
- account_customizations_repo_name: Standardmäßig ist dieser Wert auf für Benutzer festgelegt. `aft-account-customizations` AWS CodeCommit Wenn Sie ein Repository mit einem neuen Namen in CodeCommit oder in einer von AFT unterstützten VCS-Provider-Umgebung eines Drittanbieters erstellt haben, aktualisieren Sie diesen Eingabewert mit Ihrem Repository-Namen. Für BitBucket Github und GitHub Enterprise muss der Repository-Name das folgende Format haben. `[Org]/[Repo]`

- account_provisioning_customizations_repo_name: Standardmäßig ist dieser Wert auf für Benutzer festgelegt. `aft-account-provisioning-customizations` AWS CodeCommit Wenn Sie ein Repository mit einem neuen Namen in AWS CodeCommit oder in einer von AFT unterstützten VCS-Anbieterumgebung eines Drittanbieters erstellt haben, aktualisieren Sie diesen Eingabewert mit Ihrem Repository-Namen. Für BitBucket Github und GitHub Enterprise muss der Repository-Name das folgende Format `[Org]/[Repo]` haben.
- global_customizations_repo_name: Standardmäßig ist dieser Wert auf für Benutzer festgelegt. `aft-global-customizations` AWS CodeCommit Wenn Sie ein Repository mit einem neuen Namen in CodeCommit oder in einer von AFT unterstützten VCS-Provider-Umgebung eines Drittanbieters erstellt haben, aktualisieren Sie diesen Eingabewert mit Ihrem Repository-Namen. Für BitBucket Github und GitHub Enterprise muss der Repository-Name das folgende Format haben. `[Org]/[Repo]`
- 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.

Schritt 3: Stellen Sie die AWS CodeStar Verbindung für VCS-Drittanbieter her

Wenn Ihre Bereitstellung ausgeführt wird, erstellt AFT entweder die erforderlichen AWS CodeCommit Repositorys oder es stellt eine AWS CodeStar Verbindung für den von Ihnen ausgewählten VCS-Drittanbieter her. Im letzteren Fall müssen Sie sich manuell bei der Konsole des AFT-Verwaltungskontos anmelden, um die ausstehende AWS CodeStar Verbindung herzustellen. Weitere Anweisungen zum AWS CodeStar Herstellen der AWS CodeStar Verbindung finden Sie in der Dokumentation.

Datenschutz

Das -AWS Modell der geteilten Verantwortung gilt für den Datenschutz in AFT. Aus Datenschutzgründen empfehlen wir die folgenden bewährten Methoden für die Sicherheit.

- Folgen Sie den Datenschutzrichtlinien von AWS Control Tower. Details hierzu finden Sie unter Datenschutz in AWS Control Tower.

- Behalten Sie die zum Zeitpunkt der AFT-Bereitstellung generierte Terraform-Statuskonfiguration bei. Details hierzu finden Sie unter Stellen Sie AWS Control Tower Account Factory für Terraform (AFT) bereit.
- Regelmäßiges Rotieren sensibler Anmeldeinformationen gemäß den Anweisungen der Sicherheitsrichtlinie Ihrer Organisation. Beispiele für Secrets sind Terraform-Token, `git` Token usw.

Verschlüsselung im Ruhezustand

AFT erstellt Amazon S3-Buckets, Amazon SNS-Themen, Amazon SQS-Warteschlangen und Amazon-DynamoDB-Datenbanken, die im Ruhezustand mit AWS Key-Management-Service-Schlüsseln verschlüsselt werden. Von AFT erstellte KMS-Schlüssel haben die jährliche Drehung standardmäßig aktiviert. Wenn Sie die Terraform Cloud- oder Terraform Enterprise-Verteilungen von Terraform wählen, enthält AFT einen AWS Systems Manager- SecureString Parameter zum Speichern von Terraform-Token-Werten, die empfindlich sind.

AFT verwendet in beschriebene AWS Services, Komponentenservices die standardmäßig im Ruhezustand verschlüsselt sind. Weitere Informationen finden Sie in der AWS Dokumentation für jeden AWS Komponentenservice von AFT. Erfahren Sie mehr über die Datenschutzpraktiken, die von jedem Service befolgt werden.

Verschlüsselung während der Übertragung

AFT basiert standardmäßig auf den in beschriebenen AWS ServicesKomponentenservices, die die Verschlüsselung bei der Übertragung verwenden. Weitere Informationen finden Sie in der AWS Dokumentation für jeden AWS Komponentenservice von AFT. Erfahren Sie mehr über die Datenschutzpraktiken, die von jedem Service befolgt werden.

Für Terraform Cloud- oder Terraform Enterprise-Verteilungen ruft AFT eine HTTPS-Endpunkt-API für den Zugriff auf Ihre Terraform-Organisation auf. Wenn Sie sich für einen VCS-Drittanbieter entscheiden, der von AWS CodeStar Verbindungen unterstützt wird, ruft AFT eine HTTPS-Endpunkt-API auf, um Zugriff auf Ihre VCS-Anbieterorganisation zu erhalten.

Entfernen eines Kontos aus AFT

In diesem Thema wird beschrieben, wie Sie ein Konto aus AFT entfernen, 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 Verlust des Zustands führen.

Sie können ein Konto aus AFT entfernen, wenn Sie ein Konto für eine nicht mehr aktive Anwendung schließen, ein kompromittiertes Konto isolieren oder ein Konto von einer Organisation in eine andere Organisation verschieben möchten.

> **Note**
>
> Das Entfernen eines Kontos aus AFT unterscheidet sich vom Löschen eines AWS Control Tower-Kontos oder AWS-Konto. Wenn Sie ein Konto aus AFT entfernen, verwaltet AWS Control Tower das Konto weiterhin. Informationen zum Löschen eines AWS-Control-Tower-AWS-KontoKontos oder von finden Sie im Folgenden:
>
> - Heben Sie die Verwaltung eines Kontos im AWS Control Tower-Benutzerhandbuch auf.
> - Schließen eines Kontos im AWS Billing -Benutzerhandbuch.

So entfernen Sie ein Konto aus den AFT-Pipelines

Im folgenden Verfahren wird beschrieben, wie Sie ein Konto aus AFT entfernen.

1. Konto aus dem **`git`**Repository entfernen, das Kontoanforderungen speichert

   Löschen Sie in dem `git`Repository, in dem Sie Kontoanforderungen speichern, die Kontoanforderung für das Konto, das Sie aus AFT entfernen möchten.

   Wenn Sie eine Kontoanforderung aus dem Kontoanforderungs-Repository entfernen, löscht AFT die Anpassungspipeline und die Kontometadaten. Weitere Informationen finden Sie in den Versionshinweisen zu 1.8.0 für AFT auf GitHub.
2. Terraform Workspace löschen (nur für Terraform Cloud- und Terraform Enterprise-Kunden)

   Löschen Sie die Workspaces für globale Anpassungen und Kontoanpassungen für das Konto, das Sie aus AFT entfernen möchten.
3. Terraform-Status aus dem Amazon S3-Backend löschen

Löschen Sie im AFT-Verwaltungskonto alle relevanten Ordner innerhalb der Amazon S3-Buckets für das Konto, das Sie aus AFT entfernen möchten.

> **Tip**
>
> Ersetzen Sie in den folgenden Beispielen durch *012345678901* die ID-Nummer des AFT-Verwaltungskontos.

Beispiel: Terraform OSS

Wenn Sie Terraform OSS wählen, finden Sie 3 Ordner für jedes Konto in den `aft-backend-`*012345678901*`-secondary-region` Amazon S3-Buckets `aft-backend-`*012345678901*`-primary-region` und . Diese Ordner beziehen sich auf den Status der Kontoanpassungen , den Status der Anpassungspipeline und den Status der globalen Anpassungen

Beispiel: Terraform Cloud oder Terraform Enterprise

Wenn Sie Terraform Cloud oder Terraform Enterprise wählen, finden Sie einen Ordner für jedes Konto in den `aft-backend-`*012345678901*`-secondary-region` Amazon S3-Buckets `aft-backend-`*012345678901*`-primary-region` und . Diese Ordner beziehen sich auf den Status der Anpassungspipeline .

Operationelle Metriken

Standardmäßig sendet Account Factory for Terraform (AFT) anonyme Betriebsmetriken an AWS. Wir verwenden diese Daten, um zu verstehen, wie Kunden AFT verwenden, damit wir die Qualität und Features der Lösung verbessern können. Sie können die Datenerfassung deaktivieren, indem Sie einen Parameter während der AFT-Bereitstellung ändern. Wenn die Sammlung aktiviert ist, werden die folgenden Daten an gesendet AWS:

- Lösung: Die AFT-spezifische Kennung
- Version: Die Version von AFT
- Universally Unique Identifier (UUID): Zufällig generierte, eindeutige Kennung für jede AFT-Bereitstellung
- Zeitstempel: Zeitstempel der Datenerfassung

- Daten: AFT-Konfiguration und vom Kunden durchgeführte Aktionen

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 Berichtsmetriken:

- Setzen Sie den Eingabewert von `false` in Ihrer Terraform-Eingabekonfigurationsdatei `aft_metrics_reporting` auf , wie im folgenden Beispiel gezeigt, und stellen Sie AFT erneut bereit. Dieser Wert ist `true` standardmäßig auf festgelegt, wenn Sie ihn nicht explizit festlegen.

Wenn Sie das Beispiel kopieren, denken Sie daran, Ihre tatsächlichen ID- und Regionswerte für die in Zeichenfolgen angegebenen Elemente 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)

In diesem Abschnitt können Sie häufig auftretende Probleme beheben, die bei der Verwendung von Account Factory for Terraform (AFT) auftreten können.

Themen

- Allgemeine Probleme
- Probleme im Zusammenhang mit der Kontobereitstellung/Registrierung
- Probleme im Zusammenhang mit dem Aufruf von Anpassungen
- Probleme im Zusammenhang mit dem Workflow für Kontoanpassungen

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 Organizations User Guide.
  - Was ist AWS Systems Manager? im Systems Manager Manager-Benutzerhandbuch.
- Veraltete Version von Account Factory

  Wenn Sie auf ein Problem stoßen und glauben, dass es sich bei dem Problem um einen Bug handelt, stellen Sie sicher, dass Sie über die neueste Version von Account Factory verfügen. Weitere Informationen finden Sie unter Account Factory Factory-Version aktualisieren.
- Lokale Änderungen wurden am Account Factory Factory-Quellcode vorgenommen

  Account Factory ist ein Open-Source-Projekt. AWS Control Tower unterstützt den Account Factory Factory-Kerncode. Wenn Sie eine lokale Änderung am Account Factory Factory-Core-Code vornehmen, unterstützt AWS Control Tower Ihre Account Factory Factory-Bereitstellung nur nach bestem Wissen.
- Unzureichende Account Factory Factory-Rollenberechtigungen

  Account Factory erstellt IAM-Rollen und -Richtlinien, um die Bereitstellung und Anpassung von Verkäuferkonten zu verwalten. Wenn Sie diese Rollen oder Richtlinien ändern, kann die Account Factory Factory-Pipeline möglicherweise bestimmte Aktionen nicht ausführen. Weitere Informationen finden Sie unter Erforderliche Rollen.
- Konto-Repositorys wurden nicht korrekt gefüllt

Stellen Sie sicher, dass Sie die Schritte nach der Bereitstellung befolgen, bevor Sie Konten bereitstellen.

- Nach manuellem Ändern der Organisationseinheit wird keine Abweichung festgestellt

> **Note**
>
> AWS Control Tower erkennt Drift automatisch. Informationen zur Behebung von Abweichungen finden Sie unter Drift erkennen und beheben in AWS Control Tower.

Abweichungen werden nicht erkannt, wenn die Organisationseinheit (OU) manuell geändert wird. Dies ist auf den ereignisgesteuerten Charakter von Account Factory zurückzuführen. Wenn eine Kontoanfrage eingereicht wird, handelt es sich bei der von Terraform verwalteten Ressource um einen Amazon DynamoDB DynamoDB-Artikel, nicht um ein direktes Konto. Nachdem ein Element geändert wurde, wird die Anfrage in eine Warteschlange gestellt, wo AWS Control Tower sie über Service Catalog (den Service, der Kontodetails verwaltet) verarbeitet. Wenn Sie die Organisationseinheit manuell ändern, wird keine Abweichung festgestellt, da sich die Kontoanforderung nicht geändert hat.

Probleme im Zusammenhang mit der Kontobereitstellung/Registrierung

- Eine Kontoanfrage (E-Mail-Adresse/Name) ist bereits vorhanden

  Das Problem führt in der Regel zu einem Ausfall eines Service Catalog-Produkts während der Bereitstellung oder als`ConditionalCheckFailedException`.

  Sie können weitere Informationen zu dem Problem finden, 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 `aft-failure-notifications` gemeldet wurden.
- Falsch formatierte Kontoanfrage

  Vergewissern Sie sich, dass Ihre Kontoanfrage dem erwarteten Schema entspricht. Beispiele finden Sie unter terraform-aws-control_tower_account_factory on. GitHub
- Ressourcenkontingente von AWS Organizations überschritten

Stellen Sie sicher, dass Ihre Kontoanfrage die AWS Organizations Ressourcenkontingente nicht überschreitet. Weitere Informationen finden Sie unter Kontingente für AWS Organizations.

Probleme im Zusammenhang mit dem Aufruf 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 aufgenommen wurden. Weitere Informationen finden Sie unter Ein bestehendes Konto aktualisieren.
- Das Konto, auf das die Anpassungsanfrage abzielt, ist in der DynamoDB-Tabelle vorhanden**`aft-request-metadata`**, aber nicht im Kontenanforderungs-Repository

  Formatieren Sie Ihre Anfrage zum Aufruf der Anpassung so, dass das betreffende Konto 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.
  - Verwenden Sie nicht „alle“ als Ziel.
  - Es zielt nicht auf die Organisationseinheit ab, zu der das Konto gehört.
  - Das Konto wird nicht direkt ins Visier genommen.
- Falsches Token für Terraform Cloud verwendet

  Stellen Sie sicher, dass Sie das richtige Token eingerichtet haben. Terraform Cloud 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 eine Änderung an der Kontospezifikation im Repository für Kontoanfragen 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 für Kontoanpassungen

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 von kontobezogenen Metadaten aus Ihrer DynamoDB-Anforderungstabelle löschen.

Informationen zur AFT-Version 1.8.0 finden Sie unter Version 1.8.0 unter. GitHub

Informationen dazu, wie Sie Ihre Version von AFT überprüfen und aktualisieren können, finden Sie im Folgenden:

- Überprüfen Sie die AFT-Version
- Aktualisieren Sie die AFT-Version

Sie können Anpassungsanfragen auch nachverfolgen und Fehler beheben, indem Sie Amazon CloudWatch Logs Insights-Abfragen verwenden, um Protokolle zu filtern, die Ihr Zielkonto und Ihre Personalisierungsanfrage-IDs enthalten. Weitere Informationen finden Sie unter Fehlerbehebung bei der Rückverfolgung von Anfragen zur AFT-Kontoanpassung.

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.

Drift wird 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.

Bei Kontrollen, die Teil des AWS Security Hub 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.

Beispiele: Kontoabweichung und SCP-Drift werden wie folgt 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 die Abweichung korrigieren und es dann erneut ändern, erhalten Sie zwei Benachrichtigungen.
- Wenn ein Konto mehrmals zwischen denselben Quell- und Ziel-Organisationseinheiten verschoben wird, ohne dass die Abweichung zuerst behoben wurde, wird eine einzige Benachrichtigung gesendet, obwohl das Konto mehrmals zwischen diesen Organisationseinheiten gewechselt wurde.

Arten von Kontoverschiebungen

- Konto wurde zwischen Organisationseinheiten verschoben
- 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.

Arten von Richtlinien-Abweichungen

- SCP wurde aktualisiert
- SCP ist an OU angehängt
- SCP wurde von OU getrennt

- SCP ist mit dem Konto verknüpft

Weitere Informationen finden Sie unter Arten von Abweichungen in der Unternehmensführung.

Behebung von Abweichungen

Auch wenn die Erkennung automatisch erfolgt, sind zum Beheben von Abweichungen manuelle Schritte über die Konsole erforderlich.

- Viele Arten von Abweichungen können auf der Seite mit den Einstellungen für die Landezone behoben werden. Sie können im Abschnitt Versionen auf die Schaltfläche „Zurücksetzen“ klicken, um diese Arten von Abweichungen zu beheben.
- Wenn Ihre OU weniger als 300 Konten hat, können Sie Drift in Account Factory Provisioned Accounts (SCP-Drift) beheben, indem Sie auf der Seite Organisation oder der Seite mit den OU-Details die Option OU erneut registrieren auswählen.
- Möglicherweise können Sie Kontoabweichungen beheben, indem Sie Moved Member Account (Mitgliedskonto verschoben) beispielsweise ein einzelnes Konto aktualisieren. Weitere Informationen finden Sie unter Aktualisieren Sie das Konto in der Konsole.

⚠ Wenn Sie Maßnahmen ergreifen, um Drift in einer Landezone-Version zu beheben, sind zwei Verhaltensweisen möglich.

- Wenn Sie die neueste Landing Zone-Version verwenden, werden Ihre Drifted landing zone Zone-Ressourcen auf die gespeicherte AWS Control Tower Tower-Konfiguration zurückgesetzt, wenn Sie Zurücksetzen und dann Bestätigen wählen. Die Landezone-Version bleibt gleich.
- Wenn Sie nicht die neueste Version verwenden, müssen Sie Update wählen. Die landing zone wurde auf die neueste Landezonenversion aktualisiert. Die Drift wird im Rahmen dieses Prozesses behoben.

Überlegungen zu Drift- und SCP-Scans

AWS Control Tower scannt Ihre verwalteten SCPs täglich, um sicherzustellen, dass die entsprechenden Kontrollen korrekt angewendet werden und dass sie sich nicht verändert haben.

Um die SCPs abzurufen und sie 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 per Anruf prüft AWS Organizations, werden die API-Aufrufe, die AWS Control Tower tätigt, 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 unterFür die Nutzung der AWS Control Tower Tower-Konsole sind Berechtigungen erforderlich.
- Löschen Sie nicht alle zusätzlichen Organisationseinheiten: Wenn Sie die Organisationseinheit, die ursprünglich Sandbox genannt wurde, während der Einrichtung der landing zone durch AWS Control Tower löschen, befindet sich Ihre landing zone in einem Drift-Zustand, aber Sie können AWS Control Tower weiterhin verwenden. Für den Betrieb von AWS Control Tower ist mindestens eine zusätzliche Organisationseinheit erforderlich, es muss sich jedoch nicht um die Sandbox-Organisationseinheit handeln.
- Geteilte Konten nicht entfernen: Wenn Sie gemeinsame Konten aus Foundation-Organisationseinheiten entfernen, z. B. wenn Sie das Protokollierungskonto aus der Sicherheits-OU entfernen, befindet sich Ihre landing zone in einem Drift-Zustand. Die landing zone muss zurückgesetzt werden, bevor Sie die AWS Control Tower Tower-Konsole weiter verwenden können.

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.

Zulässige Änderungen außerhalb der AWS Control Tower Tower-Konsole

- 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.
- Ändern Sie den Namen der gemeinsam genutzten AWS Control Tower Tower-Konten in der Sicherheits-OU.
- 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.

Abweichungen 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 den AWS Service Catalog bereitstellen. Anweisungen finden Sie unter Konten mit AWS Service Catalog Account Factory bereitstellen .

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 Governance-Abweichungen

Abweichungen in der Unternehmensführung, auch organisatorisches Drift genannt, treten auf, wenn OUs, SCPs und Mitgliedskonten geändert oder aktualisiert werden. Folgende Arten von Governance-Abweichungen können in AWS Control Tower erkannt werden:

- Moved Member Account (Mitgliedskonto verschoben)
- Removed Member Account (Mitgliedskonto entfernt)
- Unplanned Update to Managed SCP (Außerplanmäßige Aktualisierung einer verwalteten SCP)
- SCP Attached to Member Account (SCP ist einem Mitgliedskonto zugeordnet)
- SCP Attached to Managed OU (SCP ist einer verwalteten Organisationseinheit zugeordnet)
- SCP Detached from Managed OU (SCP von verwalteter Organisationseinheit getrennt)
- Die grundlegende Organisationseinheit wurde gelöscht
- Security Hub steuert Drift
- Vertrauenswürdiger Zugriff deaktiviert

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.

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 zu Drift finden Sie im Abschnitt „Erforderliche Rollen nicht löschen“Arten von Abweichungen, die sofort behoben werden müssen.

AWS Control Tower sucht nicht nach Abweichungen in Bezug auf andere Services, die mit dem Verwaltungskonto funktionieren CloudTrail CloudWatch, einschließlich,, IAM Identity Center AWS CloudFormation AWS Config,, usw. Bei Konten von Kindern ist keine Erkennung von Abweichungen verfügbar, da diese Konten durch präventive obligatorische Kontrollen geschützt sind.

Es werden jedoch Abweichungen in Bezug auf Kontrollen gemeldet, die Teil des AWS Security Hub Service-Managed Standard sind: AWS Control Tower.

Moved Member Account (Mitgliedskonto verschoben)

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. Das Folgende ist ein Beispiel für die Amazon SNS SNS-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 300 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 300 Konten auftritt, können Sie sie wie folgt beheben:

- Navigieren Sie in der AWS Control Tower Tower-Konsole zur Organisationsseite, 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 Sie dann Erneut registrieren für die Organisationseinheit, 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 Aktualisierung und Verschiebung von Accountfactory-Konten mit AWS Control Tower oder mit AWS Service Catalog.

  > **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 300 Konten auftritt, kann die Auflösung der Abweichung davon abhängen, welcher Kontotyp verschoben wurde, wie in den nächsten Absätzen erläutert. Weitere Informationen finden Sie unter Aktualisieren Ihrer Landing Zone.

  - Wenn ein von Account Factory bereitgestelltes Konto verschoben wird — In einer OU mit weniger als 300 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 300 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 Aktualisierung durch eine erneute Registrierung der Organisationseinheit nicht durchgeführt wird. Weitere Informationen finden Sie unter Aktualisierung und Verschiebung von Accountfactory-Konten mit AWS Control Tower oder mit AWS Service Catalog.

  - 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 Aktualisieren Ihrer Landing Zone.

> **Veralteter Feldname**
>
> Der Feldname `MasterAccountID` wurde geändert, sodass er den Richtlinien `ManagementAccountID` entspricht AWS . Der alte Name ist veraltet. Ab 2022 funktionieren Skripts, die den veralteten Feldnamen enthalten, nicht mehr.

Removed Member Account (Mitgliedskonto 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 Amazon SNS SNS-Benachrichtigung, wenn diese Art von Drift 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 Aktualisierung und Verschiebung von Accountfactory-Konten mit AWS Control Tower oder mit AWS Service Catalog.
- 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.

Unplanned Update to Managed SCP (Außerplanmäßige Aktualisierung einer verwalteten 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. Das Folgende ist ein Beispiel für die Amazon SNS SNS-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 eine solche Abweichung in einer Organisationseinheit mit bis zu 300 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 Aktualisieren Ihrer Landing Zone.

Wenn diese Art von Abweichung in einer Organisationseinheit mit mehr als 300 Konten auftritt, beheben Sie das Problem, indem Sie Ihre landing zone aktualisieren. Weitere Informationen finden Sie unter Aktualisieren Ihrer Landing Zone.

SCP Attached to Managed OU (SCP ist einer verwalteten Organisationseinheit zugeordnet)

Diese Art von Abweichung kann auftreten, wenn ein SCP für eine Steuerung an eine andere Organisationseinheit angehängt ist. Dieses Ereignis tritt besonders häufig auf, wenn Sie von außerhalb der AWS Control Tower Tower-Konsole an Ihren Organisationseinheiten arbeiten. Das Folgende ist ein Beispiel für die Amazon SNS SNS-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)' has been attached to 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-ou'",
  "ManagementAccountId" : "012345678912",
  "OrganizationId" : "o-123EXAMPLE",
  "DriftType" : "SCP_ATTACHED_TO_OU",
  "RemediationStep" : "Update Control Tower Setup",
  "OrganizationalUnitId" : "ou-0123-1EXAMPLE",
  "PolicyId" : "p-tEXAMPLE"
}
```

Auflösung

Wenn eine solche Abweichung in einer Organisationseinheit mit bis zu 300 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 Aktualisieren Ihrer Landing Zone.

Wenn diese Art von Abweichung in einer Organisationseinheit mit mehr als 300 Konten auftritt, beheben Sie das Problem, indem Sie Ihre landing zone aktualisieren. Weitere Informationen finden Sie unter Aktualisieren Ihrer Landing Zone.

SCP Detached from Managed OU (SCP von verwalteter 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. Das Folgende ist ein Beispiel für die Amazon SNS SNS-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)' 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 eine solche Abweichung in einer Organisationseinheit mit bis zu 300 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 unterAktualisieren Ihrer Landing Zone.

Wenn diese Art von Abweichung in einer Organisationseinheit mit mehr als 300 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 unterAktualisieren Ihrer Landing Zone.

SCP Attached to Member Account (SCP ist einem Mitgliedskonto zugeordnet)

Diese Art von Abweichung kann auftreten, wenn ein SCP für eine Kontrolle mit einem Konto in der Organisationskonsole verknüpft ist. Guardrails und ihre SCPs können über die AWS Control Tower Tower-Konsole für OUs aktiviert (und somit auf alle registrierten Konten einer OU angewendet) werden. Das Folgende ist ein Beispiel für die Amazon SNS SNS-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)' has been attached to the member account 'account-
email@amazon.com (012345678909)'. For more information, including steps to resolve this
 issue, see 'https://docs.aws.amazon.com/console/controltower/scp-detached-account'",
  "ManagementAccountId" : "012345678912",
  "OrganizationId" : "o-123EXAMPLE",
  "DriftType" : "SCP_ATTACHED_TO_ACCOUNT",
  "RemediationStep" : "Re-register this organizational unit (OU)",
  "AccountId" : "012345678909",
  "PolicyId" : "p-tEXAMPLE"
}
```

Auflösung

Diese Art von Abweichung tritt eher auf dem Konto als auf der Organisationseinheit auf.

Wenn diese Art von Abweichung bei Konten in einer Foundational OU, wie der Security OU, auftritt, besteht die Lösung darin, Ihre landing zone zu aktualisieren. Weitere Informationen finden Sie unter Aktualisieren Ihrer Landing Zone.

Wenn eine solche Abweichung in einer Organisationseinheit auftritt, die nicht zu den Grundlagen gehört und bis zu 300 Konten hat, können Sie sie wie folgt beheben:

- Trennen des AWS Control Tower SCP vom Account Factory-Konto.
- 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.

Wenn diese Art von Abweichung in einer Organisationseinheit mit mehr als 300 Konten auftritt, können Sie versuchen, das Problem zu beheben, indem Sie die werkseitige Konfiguration des Kontos für das Konto aktualisieren. Es ist möglicherweise nicht möglich, das Problem erfolgreich zu lösen. Weitere Informationen finden Sie unter Aktualisieren Ihrer 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 Amazon SNS SNS-Benachrichtigung, die Sie möglicherweise erhalten, wenn diese Art von Abweichung 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 steuert Drift

Diese Art von Abweichung tritt auf, wenn eine Steuerung, die Teil des AWS Security Hub Service-Managed Standard: AWS Control Tower ist, einen Drift-Status meldet. Der AWS Security Hub Service selbst meldet keinen Drift-Status für diese Kontrollen. Stattdessen sendet der Service seine Ergebnisse an AWS Control Tower.

Kontrollabweichungen im Security Hub können auch festgestellt werden, wenn AWS Control Tower seit mehr als 24 Stunden kein Status-Update von Security Hub erhalten hat. Wenn diese Ergebnisse nicht wie erwartet eingehen, überprüft AWS Control Tower, ob die Kontrolle nicht stimmt. Das folgende Beispiel zeigt eine Amazon SNS SNS-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" : "PYBETSAGNUZB",
"ControlName" : "EBS snapshots should not be publicly restorable",
"ApiControlIdentifier" : "arn:aws:controltower:us-east-1::control/PYBETSAGNUZB",
"Region" : "us-east-1"
}
```

Auflösung

Bei Organisationseinheiten mit weniger als 300 Konten besteht die Lösung darin, die Organisationseinheit erneut zu registrieren, wodurch die Steuerung auf den ursprünglichen Status zurückgesetzt wird. Für jede 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: Amazon SNS SNS-Benachrichtigung

Im Folgenden finden Sie ein Beispiel für die Amazon SNS SNS-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.

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 von AWS Control Tower ändern. Der häufigste Ort, an dem Ressourcen außerhalb von AWS Control Tower geändert werden, ist die AWS Organizations Konsole. In diesem Thema wird beschrieben, wie Sie Änderungen an den 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 Tower-Konsole führt dazu, dass die Konsole nicht mehr synchron ist. Viele Änderungen können automatisch abgeglichen werden. Bestimmte Änderungen erfordern ein Zurücksetzen Ihrer landing zone, um die in der AWS Control Tower Tower-Konsole angezeigten Informationen zu aktualisieren.

Im Allgemeinen führen Änderungen, die Sie außerhalb der AWS Control Tower Tower-Konsole an den AWS Control Tower Tower-Ressourcen vornehmen, zu einer behebbaren Abweichung in Ihrer landing zone. Weitere Informationen zu diesen Änderungen finden Sie unter Reparierbare Änderungen an Ressourcen.

Aufgaben, für die die landing zone zurückgesetzt werden muss

- Löschen der Sicherheits-OU (Ein Sonderfall, der nicht leichtfertig durchgeführt werden sollte.)
- Ein gemeinsam genutztes Konto aus der Sicherheits-OU entfernen (nicht empfohlen.)
- Aktualisierung, Anfügen oder Trennen eines mit der Sicherheits-OU verknüpften SCP

Änderungen, die automatisch von AWS Control Tower aktualisiert werden

- Ändern der E-Mail-Adresse eines angemeldeten Kontos
- Umbenennen eines angemeldeten Kontos
- Erstellung einer neuen Organisationseinheit (OU) der obersten Ebene
- Umbenennen einer registrierten Organisationseinheit
- 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 Sicherheits-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 dadurch in Einklang gebracht werden. Weitere Informationen zur Aktualisierung eines bereitgestellten Produkts finden Sie in der Dokumentation unter Aktualisieren bereitgestellter Produkte. AWS Service Catalog

Verweis auf Ressourcen außerhalb von AWS Control Tower

Wenn Sie neue Organisationseinheiten und Konten außerhalb von AWS Control Tower erstellen, werden diese nicht von AWS Control Tower verwaltet, 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 Seite Organisation angezeigt, unterliegen jedoch nicht den AWS Control Tower Tower-Kontrollen.

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 bei AWS Control Tower registrierten Organisationseinheit gehören, werden auf der Seite Organisation angezeigt. Konten, die nicht zu einer registrierten Organisationseinheit gehören, können über die AWS Organizations Konsole eingeladen werden. Durch diese Einladung zum Beitritt wird das Konto nicht bei AWS Control Tower registriert und auch nicht die AWS Control Tower-Governance auf das Konto ausgedehnt. Um die Verwaltung durch die Registrierung des Kontos zu erweitern, rufen Sie die Organisationsseite oder die Kontodetailseite in AWS Control Tower auf und wählen Sie Konto registrieren aus.

Externes Ändern von AWS Control Tower Tower-Ressourcennamen

Sie können die Namen Ihrer Organisationseinheiten (OUs) und Konten außerhalb der AWS Control Tower Tower-Konsole ändern, und die Konsole wird automatisch aktualisiert, um diese Änderungen widerzuspiegeln.

Umbenennen einer OU

AWS Organizations In können Sie den Namen einer Organisationseinheit 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 Tower-Konsole die Namensänderung automatisch wider. Wenn Sie Ihre Konten jedoch über 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 der Services für die grundlegenden und zusätzlichen Organisationseinheiten. Sie können diese Art von Abweichung auf der Seite mit den Landingzone-Einstellungen beheben. Weitere Informationen finden Sie im Abschnitt „Drift lösen“ unterAbweichungen im AWS Control Tower erkennen und beheben.

AWS Control Tower zeigt die Namen der Organisationseinheiten auf der Seite Organisation im AWS Control Tower 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 Billing and Cost Management Konsole geändert werden kann. Wenn Sie ein Konto umbenennen, das bei AWS Control Tower registriert ist, wird die Namensänderung automatisch in AWS Control Tower widergespiegelt. Weitere Informationen zur Änderung 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 Security OU löschen, wird eine Seite mit einer Fehlermeldung angezeigt, auf der Sie aufgefordert werden, Ihre landing zone zurückzusetzen. Sie müssen Ihre landing zone zurücksetzen, bevor Sie andere Aktionen in AWS Control Tower ausführen können.

- Sie können in der AWS Control Tower Tower-Konsole keine Aktionen ausführen und keine neuen Konten erstellen, AWS Service Catalog bis der Reset abgeschlossen ist.
- Sie werden nicht in der Lage sein, auf der Seite mit den Einstellungen für die Landingzone die Schaltfläche „Zurücksetzen“ zu sehen.

In diesem Fall erstellt der Vorgang zum Zurücksetzen der landing zone eine neue Sicherheits-OU und verschiebt die beiden gemeinsam genutzten Konten in die neue Sicherheits-OU. AWS Control Tower

markiert die Konten Log Archive und Audit als verschoben. Derselbe Prozess behebt die Abweichung bei diesen Konten.

Wenn Sie feststellen, dass Sie die Sicherheits-OU löschen müssen, sollten Sie Folgendes wissen:

Bevor Sie die Sicherheits-OU löschen können, müssen Sie sicherstellen, dass sie keine Konten enthält. Insbesondere müssen Sie die Konten Log Archive und Audit aus der Organisationseinheit entfernen. Es wird empfohlen, diese Konten in eine andere OU zu verschieben.

> **Note**
>
> Das Löschen Ihrer Sicherheits-OU darf nicht ohne gebührende Berücksichtigung 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 entfernen. Wenn Sie versehentlich ein geteiltes Konto entfernt haben, können Sie die Schritte zur Problembehebung in diesem Abschnitt befolgen, um das Konto wiederherzustellen.

- Von der AWS Control Tower Tower-Konsole aus: Um den Behebungsprozess zu starten, folgen Sie den halbmanuellen Behebungsschritten. Stellen Sie sicher, dass der Benutzer oder die Rolle, die Sie für den Zugriff auf die AWS Control Tower Tower-Konsole verwenden, über Ausführungsberechtigungen verfügt`organizations:InviteAccountToOrganization`. Wenn Sie nicht über solche Berechtigungen verfügen, folgen Sie den Schritten zur manuellen Problembehebung, die sowohl die AWS Control Tower Tower-Konsole als auch die AWS Organizations Konsole verwenden.
- Ausgehend von der AWS Organizations Konsole: Dieser Behebungsprozess ist ein etwas längerer, vollständig manueller Vorgang. Wenn Sie die manuellen Schritte zur Problembehebung befolgen, wechseln Sie zwischen der AWS Organizations Konsole und der AWS Control Tower Tower-Konsole. Für die Arbeit in 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 Tower-Konsole arbeiten, benötigen Sie einen Benutzer oder eine Rolle mit der `AWSControlTowerServiceRolePolicy` verwalteten Richtlinie oder einer gleichwertigen Richtlinie und die Erlaubnis, alle AWS Control Tower Tower-Aktionen auszuführen (Controltower: *).

- Wenn das Konto durch die Schritte zur Problembehebung nicht wiederhergestellt werden konnte, wenden Sie sich an. AWS Support

Die Ergebnisse der Entfernung 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 ist 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: Die Aktualisierungen und der Reset von AWS Control Tower schlagen fehl.

So stellen Sie ein gemeinsam genutztes Konto mithilfe der AWS Control Tower Tower-Konsole wieder her (halbmanuelles Verfahren)

1. Melden Sie sich unter https://console.aws.amazon.com/controltower bei der AWS Control Tower Tower-Konsole an. 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 Verfahren zur manuellen Problembehebung, das weiter unten in diesem Thema beschrieben wird.
2. Wählen Sie auf der Seite Landingzone-Drift erkannt die Option Erneut einladen aus, um das Entfernen eines gemeinsamen Kontos zu korrigieren, indem Sie das gemeinsame Konto 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:

   - Melden Sie sich bei dem geteilten Konto an, das entfernt wurde, und gehen Sie 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 sich das geteilte Konto, das entfernt wurde, nicht in einer anderen Organisation befindet, melden Sie sich bei dem Konto an, öffnen Sie die AWS Organizations Konsole und navigieren Sie zu Einladungen.

4. Melden Sie sich erneut beim Verwaltungskonto an oder laden Sie die AWS Control Tower Tower-Konsole neu, falls sie bereits geöffnet ist. Sie werden die Drift-Seite für die Landing Zone sehen. Wählen Sie Reset, um die landing zone zu reparieren.
5. Warten Sie, bis der Reset-Vorgang abgeschlossen ist.

Wenn die Problembehebung erfolgreich ist, befindet sich das gemeinsam genutzte Konto in einem normalen Zustand und weist die Konformität auf.

Wenn das Konto durch die Schritte zur Problembehebung nicht wiederhergestellt wird, wenden Sie sich an. AWS Support

So stellen Sie ein gemeinsam genutztes Konto mithilfe des AWS Control Tower und der AWS Organizations Konsolen wieder her (manuelle Behebung)

1. Melden Sie sich bei der AWS Organizations Konsole an unterhttps://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 wieder in die Organisation ein. Informationen zu den Anforderungen, Voraussetzungen und dem Verfahren für das Einladen eines Kontos finden Sie im AWS Organizations Benutzerhandbuch unter Ein AWS Konto in Ihre Organisation einladen. AWS Organizations
3. Melden Sie sich bei dem geteilten Konto an, das entfernt wurde, und gehen Sie dann zu https://console.aws.amazon.com/organizations/home#/invites, um die Einladung anzunehmen.
4. Melden Sie sich erneut beim Verwaltungskonto an.

5. Melden Sie sich bei der AWS Control Tower Tower-Konsole als Benutzer oder Rolle mit der `AWSControlTowerServiceRolePolicy` verwalteten Richtlinie oder einer gleichwertigen Richtlinie und den Berechtigungen zur Ausführung aller AWS Control Tower Tower-Aktionen an (Controltower: *).
6. Sie sehen die Drift-Seite für die landing zone mit einer Option zum Zurücksetzen der Landezone. Wählen Sie Reset, um die landing zone zu reparieren.
7. Warten Sie, bis der Reset-Vorgang abgeschlossen ist.

Wenn die Problembehebung erfolgreich ist, befindet sich das gemeinsam genutzte Konto in einem normalen Zustand und weist die Konformität auf.

Wenn das Konto durch die Schritte zur Problembehebung 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, aber Account Factory aktualisiert sie 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 Konsolenerfahrung erforderlich ist. Daher werden E-Mail-Adressen für gemeinsam genutzte Konten und andere Konten aktualisiert und konsistent in AWS Control Tower 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.

Anwenden externer Regeln AWS Config

AWS Control Tower zeigt den Compliance-Status aller AWS Config Regeln an, die in den bei AWS Control Tower registrierten Organisationseinheiten implementiert wurden, einschließlich Regeln, die außerhalb der AWS Control Tower Tower-Konsole aktiviert wurden.

Löschen von AWS Control Tower-Ressourcen außerhalb von AWS Control Tower

Sie können OUs und Konten in 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)

Darin 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 Organisationseinheit 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 bereitstellen können.

Löschen eines angemeldeten Kontos aus einer Organisationseinheit

Wenn Sie ein registriertes Konto löschen, erhält AWS Control Tower eine Benachrichtigung und aktualisiert es, 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).

Kontrollieren von 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 über vorhandene OUs und Konten verfügen, die außerhalb von AWS Control Tower erstellt wurden, können Sie diese auch in die AWS Control Tower-Governance integrieren.

Bei vorhandenen - AWS Organizations und - 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 Registriere ein vorhandenes AWS-Konto.

Terminologie

- Wenn Sie eine vorhandene Organisation in AWS Control Tower einbinden, wird dies als Registrierung der Organisation oder Erweiterung der Unternehmensführung bezeichnet.
- Wenn Sie ein AWS Konto in AWS Control Tower einbinden, wird dies als Registrierung des Kontos bezeichnet.

Anzeigen Ihrer OUs und Konten

Auf der Seite AWS Control Tower Organization können Sie alle OUs in Ihrem anzeigen AWS Organizations, einschließlich der OUs, die bei AWS Control Tower registriert sind, und derjenigen, die nicht registriert sind. Sie können verschachtelte OUs als Teil der Hierarchie anzeigen. Eine einfache Möglichkeit, Ihre Organisationseinheiten auf der Seite Organisation anzuzeigen, besteht darin, Organisationseinheiten nur aus der Dropdownliste oben rechts auszuwählen.

Auf der Seite Organisation werden alle Konten in Ihrer Organisation aufgeführt, unabhängig von der Organisationseinheit oder dem Registrierungsstatus in AWS Control Tower. Eine einfache Möglichkeit, Ihre Konten auf der Seite Organisation anzuzeigen, besteht darin, Konten nur aus der Dropdownliste oben rechts auszuwählen. Sie können Konten einzeln innerhalb der OUs anzeigen, aktualisieren und registrieren, wenn die Konten die Voraussetzungen für die Registrierung erfüllen.

Wenn Sie keine Filterung auswählen, werden auf der Seite Organisation Ihre Konten und OUs 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 Seite Organisation finden Sie in der Videoanleitung.

Video-Anleitung

In diesem Video (4:01) wird beschrieben, wie Sie mit der Seite Organisation in 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.

Video-Walkthrough zum Arbeiten mit der Organisationsseite in AWS Control Tower.

Themen

- Registrieren Sie eine bestehende Organisationseinheit bei AWS Control Tower
- Registriere ein vorhandenes AWS-Konto

Erweitern der Governance auf eine bestehende Organisation

Sie können AWS Control Tower Governance zu einer vorhandenen Organisation hinzufügen, indem Sie eine Landing Zone (LZ) einrichten, wie im AWS Control Tower-Benutzerhandbuch unter Erste Schritte, Schritt 2 beschrieben.

Folgendes ist zu erwarten, wenn Sie Ihre Landing Zone von AWS Control Tower in einer bestehenden Organisation einrichten.

- Sie können pro AWS Organizations Organisation eine Landing Zone haben.
- AWS Control Tower verwendet das Verwaltungskonto Ihrer vorhandenen AWS Organizations Organisation als Verwaltungskonto. Es wird kein neues Verwaltungskonto benötigt.
- AWS Control Tower richtet zwei neue Konten in einer registrierten Organisationseinheit ein: ein Audit-Konto und ein Protokollierungskonto.
- Die Service Limits Ihrer Organisation müssen die Erstellung dieser beiden zusätzlichen Konten ermöglichen.
- Nachdem Sie Ihre Landing Zone gestartet oder eine Organisationseinheit registriert haben, gelten die Steuerelemente von AWS Control Tower automatisch für alle registrierten Konten in dieser Organisationseinheit.
- Sie können zusätzliche vorhandene AWS Konten in eine Organisationseinheit registrieren, die von AWS Control Tower geregelt wird, sodass Kontrollen für diese Konten gelten.

- Sie können weitere OUs in AWS Control Tower hinzufügen und vorhandene OUs registrieren.

Weitere Voraussetzungen für die Registrierung und Registrierung finden Sie unter Erste Schritte mit AWS Control Tower.

Im Folgenden finden Sie weitere Informationen darüber, wie AWS Control Tower-Steuerelemente nicht für Ihre OUs in AWS-Organisationen gelten, für die keine Landing Zones für AWS Control Tower eingerichtet sind:

- Neue Konten, die außerhalb von AWS Control Tower Account Factory erstellt wurden, sind nicht an die Kontrollen der registrierten Organisationseinheit gebunden.
- Neue Konten, die in OUs 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 Registriere ein vorhandenes AWS-Konto.
- Zusätzliche bestehende Organisationen, bestehende Konten und alle neuen OUs 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 Organisationseinheit separat oder registrieren das Konto.

Weitere Informationen zum Anwenden von AWS Control Tower auf bestehende OUs und Konten finden Sie unter Registrieren Sie eine bestehende Organisationseinheit bei AWS Control Tower.

Eine Übersicht über die Einrichtung einer Landing Zone von AWS Control Tower in Ihrer bestehenden Organisation finden Sie im Video im nächsten Abschnitt.

> **Note**
>
> Während der Einrichtung führt AWS Control Tower Vorabprüfungen durch, um häufige Probleme zu vermeiden. Wenn Sie derzeit jedoch die AWS Landing Zone-Lösung für verwenden, wenden Sie sich an Ihren AWS Lösungsarchitekten AWS Organizations, bevor Sie versuchen, AWS Control Tower in Ihrer Organisation zu aktivieren, um festzustellen, ob AWS Control Tower Ihre aktuelle Bereitstellung der Landing Zone beeinträchtigen kann. Weitere Informationen Was ist, wenn das Konto die Voraussetzungen nicht erfüllt? zum Verschieben von Konten von einer Landing Zone zu einer anderen finden Sie unter .

Video: Aktivieren einer Landing Zone in vorhandenen AWS Organizations

In diesem Video (7:48) wird beschrieben, wie Sie eine Landing Zone von AWS Control Tower in vorhandenen AWS Organizations Strukturen einrichten und aktivieren. 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 von AWS Control Tower für bestehende Organisationen

Überlegungen zu IAM Identity Center und bestehenden Organisationen

- Wenn AWS IAM Identity Center (IAM Identity Center) bereits eingerichtet ist, muss die Heimatregion des AWS Control Tower mit der Region des IAM Identity Center übereinstimmen.
- 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 ist, ändert AWS Control Tower die vorhandene Konfiguration nicht. Weitere Details finden Sie unter Überlegungen für AWS IAM Identity Center (IAM Identity Center)-Kunden.

Zugriff auf andere - AWS Services

Nachdem Sie Ihre Organisation in die AWS Control Tower-Governance integriert haben, haben Sie weiterhin Zugriff auf alle AWS Services, die über verfügbar sind AWS Organizations, mithilfe der AWS Organizations Konsole und APIs APIs. Weitere Informationen finden Sie unter Zugehörige AWS-Services.

Verschachtelte Organisationseinheiten im AWS Control Tower

In diesem Kapitel werden die Erwartungen und Überlegungen aufgeführt, die Sie bei der Arbeit mit verschachtelten Organisationseinheiten in AWS Control Tower beachten sollten. In den meisten Fällen entspricht die Arbeit mit verschachtelten Organisationseinheiten der Arbeit mit einer flachen OU-Struktur. Die Funktionen „Registrieren“ und „Erneut registrieren“ funktionieren mit verschachtelten Organisationseinheiten, mit Ausnahme der geänderten Verhaltensweisen, auf die in diesem Kapitel eingegangen wird.

Video-Anleitung

In diesem Video (4:46) wird beschrieben, wie verschachtelte OU-Bereitstellungen in 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.

Videoanleitung zur Verwaltung verschachtelter Organisationseinheiten in AWS Control Tower.

Anleitungen zu bewährten Methoden für verschachtelte Organisationseinheiten und Ihre landing zone finden Sie im Blogbeitrag Organizing your AWS Control Tower landing zone with Nested OUs.

Erweitern Sie von einer flachen OU-Struktur zu einer verschachtelten OU-Struktur

Wenn Sie Ihre AWS Control Tower Tower-Landezone 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 die gewünschte verschachtelte OU-Struktur in AWS Control Tower.
2. Gehen Sie zur AWS Organizations Konsole und verwenden Sie deren Funktion zur Massenverschiebung, um die Konten von der Quell-OU (flach) in die Ziel-OU (verschachtelt) zu verschieben. So geht's:
   a. Gehen Sie zu der Organisationseinheit, von der Sie Konten verschieben möchten.
   b. Wählen Sie alle Konten in der Organisationseinheit aus.
   c. Wählen Sie „Verschieben“.

   > **Note**
   >
   > Dieser Schritt muss in der AWS Organizations In-Konsole ausgeführt werden, da AWS Control Tower keine Move-Funktion hat.

3. Gehen Sie zur verschachtelten Organisationseinheit in AWS Control Tower und registrieren Sie sie oder registrieren Sie sie erneut. Alle Konten in der verschachtelten Organisationseinheit werden registriert.
   - Wenn Sie die OU in AWS Control Tower erstellt haben, registrieren Sie die OU erneut.
   - Wenn Sie die OU in erstellt haben AWS Organizations, registrieren Sie die OU 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 Tower-Konsole aus.

Vorabprüfungen für die Registrierung verschachtelter Organisationseinheiten

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 von Organisationseinheiten der obersten Ebene oder verschachtelten Organisationseinheiten durchgeführt. Weitere Informationen finden Sie unter Häufige Ursachen für Fehler bei der Registrierung oder erneuten Registrierung.

- Wenn alle Vorabprüfungen erfolgreich sind, beginnt AWS Control Tower automatisch mit der Registrierung Ihrer Organisationseinheit.
- Wenn irgendwelche Vorabprüfungen fehlschlagen, stoppt AWS Control Tower den Registrierungsprozess und stellt Ihnen eine Liste mit Problemen zur Verfügung, die behoben werden müssen, bevor Sie Ihre Organisationseinheit registrieren können.

Verschachtelte Organisationseinheiten und Rollen

AWS Control Tower stellt die `AWSControlTowerExecution` Rolle für Konten unter der Ziel-OU und für Konten in allen OUs bereit, die unter der Ziel-OU verschachtelt sind, auch wenn Sie nur die Ziel-OU registrieren möchten. Diese Rolle gewährt jedem Benutzer des Verwaltungskontos Administratorrechte für jedes Konto, das diese Rolle besitzt. `AWSControlTowerExecution` Die Rolle kann verwendet werden, um Aktionen auszuführen, die normalerweise von AWS Control Tower Controls nicht zugelassen würden.

Sie können diese Rolle aus nicht registrierten Konten löschen, 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 darüber, wie Sie den Rollenzugriff einschränken können, 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.
- Registrierte Mitgliedskonten werden erneut registriert.
- Erstellt ein IAM Identity Center-Login für neu registrierte Mitgliedskonten.
- Aktualisiert bestehende registrierte Mitgliedskonten, um Ihre Änderungen in der landing zone widerzuspiegeln.
- Aktualisiert die Steuerelemente, die für diese Organisationseinheit und ihre Mitgliedskonten konfiguriert sind.

Überlegungen zur Registrierung verschachtelter Organisationseinheiten

- Sie können eine Organisationseinheit nicht unter der Kernorganisationseinheit (Sicherheits-OU) registrieren.
- Verschachtelte Organisationseinheiten müssen separat registriert werden.
- Sie können eine Organisationseinheit nur registrieren, wenn ihre übergeordnete Organisationseinheit registriert ist.
- Sie können eine Organisationseinheit nur registrieren, wenn alle Organisationseinheiten, die sich weiter oben in der Struktur befinden, zu einem bestimmten Zeitpunkt erfolgreich registriert wurden (einige wurden möglicherweise gelöscht).
- Sie können eine Organisationseinheit registrieren, die sich unter einer geänderten höheren Organisationseinheit befindet, aber die Abweichung wird durch diese Aktion nicht behoben.

Einschränkungen verschachtelter Organisationseinheiten

- Organisationseinheiten können maximal 5 Ebenen tief unter dem Stamm verschachtelt werden.
- Verschachtelte Organisationseinheiten unter der Ziel-Organisationseinheit müssen separat registriert oder erneut registriert werden.
- Wenn sich die Ziel-Organisationseinheit in der Hierarchie auf Stufe 2 oder darunter befindet, d. h. wenn es sich nicht um eine Organisationseinheit der obersten Ebene handelt, werden präventive Kontrollen, die für höhere Organisationseinheiten aktiviert sind, automatisch für diese Organisationseinheit und alle Organisationseinheiten unterhalb dieser Organisationseinheit durchgesetzt.
- Fehler bei der Registrierung von Organisationseinheiten werden in der Hierarchiestruktur nicht nach oben übertragen. Einzelheiten zum Status verschachtelter Organisationseinheiten finden Sie auf der Seite mit den OU-Details der übergeordneten Organisationseinheit.
- Fehler bei der Registrierung von Organisationseinheiten werden in der Hierarchiestruktur nicht nach unten übertragen.
- AWS Control Tower ändert Ihre VPC-Einstellungen für neue oder bestehende Konten nicht.

Verschachtelte Organisationseinheiten und Konformität

Von der AWS Control Tower Tower-Konsole aus können Sie Organisationseinheiten und Konten, die nicht konform sind, auf der Seite Organisation anzeigen, sodass Sie die Einhaltung von Vorschriften in größerem Umfang nachvollziehen können.

Überlegungen zur Einhaltung von Vorschriften für verschachtelte Organisationseinheiten und Konten

- Die Konformität einer Organisationseinheit wird nicht anhand der Konformität der ihr untergeordneten Organisationseinheiten bestimmt.
- Der Konformitätsstatus eines Steuerelements wird für alle Organisationseinheiten berechnet, für die das Steuerelement aktiviert ist, einschließlich verschachtelter Organisationseinheiten. Sehen Sie sich den AWS Control Tower Tower-Compliance-Status für Organisationseinheiten und Konten an.
- Eine Organisationseinheit wird nur dann als nicht konform angezeigt, wenn sie Konten hat, die nicht konform sind, unabhängig davon, wo sich die Organisationseinheit in der OU-Hierarchie befindet.

- Wenn eine verschachtelte Organisationseinheit nicht konform ist, wird ihre übergeordnete Organisationseinheit nicht automatisch als nicht konform betrachtet.
- Auf der Seite mit den OU-Details oder den Kontodetails können Sie eine Liste der nicht konformen Ressourcen einsehen, die möglicherweise dazu führen, dass Ihre Organisationseinheiten oder Konten den Status „Nicht konform“ aufweisen.

Verschachtelte Organisationseinheiten und Drift

In bestimmten Situationen kann Drift die Registrierung verschachtelter Organisationseinheiten verhindern.

Erwartungen an Drift- und verschachtelte Organisationseinheiten

- Sie können Steuerungen für Organisationseinheiten mit abweichenden übergeordneten Organisationseinheiten aktivieren, jedoch nicht direkt für geänderte Organisationseinheiten.
- In einer geänderten Organisationseinheit können Sie die detektivische Kontrolle aktivieren, sofern es sich nicht um eine geänderte Organisationseinheit der obersten Ebene handelt.
- Obligatorische Kontrollen sind nur für Organisationseinheiten der obersten Ebene aktiviert. Obligatorische Kontrollen werden übersprungen, wenn Sie eine verschachtelte Organisationseinheit registrieren.
- Ein obligatorisches Steuerelement schützt AWS Config Ressourcen. Daher muss sich dieses Steuerelement in einem unveränderlichen Zustand befinden, um verschachtelte Organisationseinheiten registrieren zu können. Bei Abweichung blockiert AWS Control Tower die Registrierung verschachtelter Organisationseinheiten.
- Wenn sich die Organisationseinheit der obersten Ebene ändert, kann es sein, dass die Kontrolle, die AWS Config Ressourcen schützt, nicht stimmt. In dieser Situation blockiert 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 für eine registrierte Organisationseinheit aktivieren, verhalten sich präventive und detektive Kontrollen unterschiedlich. Bei verschachtelten Organisationseinheiten verhalten sich proaktive Kontrollen ähnlich wie detektive Kontrollen.

Präventive Kontrollen

- Präventive Kontrollen werden für verschachtelte Organisationseinheiten durchgesetzt.
- Obligatorische präventive Kontrollen werden für alle Konten der Organisationseinheit und ihrer verschachtelten Organisationseinheiten durchgesetzt.
- Präventive Kontrollen wirken sich auf alle Konten und Organisationseinheiten aus, die unter der Ziel-OU verschachtelt sind, auch wenn diese Konten und Organisationseinheiten nicht registriert sind.

Detective und proaktive Kontrollen

- Verschachtelte Organisationseinheiten übernehmen nicht automatisch detektive oder proaktive Kontrollen. Diese müssen separat aktiviert werden.
- Detective und proaktive Kontrollen werden nur für registrierte Konten in den Betriebsregionen Ihrer Landezone eingesetzt.

Kontrollstatus und Vererbung aktiviert

Sie können die geerbten Steuerelemente für jede Organisationseinheit auf der Seite mit den OU-Details anzeigen.

> **Tip**
>
> Sie können die Vererbung von Steuerelementen nutzen, um das SCP-Kontingent einer Organisationseinheit einzuhalten. Sie können beispielsweise ein Steuerelement auf der obersten Ebene einer OU-Hierarchie aktivieren, anstatt es direkt für eine verschachtelte Organisationseinheit zu aktivieren.

Vererbter Status

- Der Status Vererbt gibt an, dass das Steuerelement nur durch Vererbung aktiviert wurde und nicht direkt auf die Organisationseinheit angewendet wurde.
- Der Status Aktiviert bedeutet, dass die Steuerung in dieser Organisationseinheit durchgesetzt wird, unabhängig von ihrem Status in anderen Organisationseinheiten.
- Der Status Fehlgeschlagen bedeutet, dass die Steuerung für diese Organisationseinheit nicht durchgesetzt wird, unabhängig von ihrem Status in anderen Organisationseinheiten.

> **Note**
>
> Der Status Vererbt gibt an, dass das Steuerelement auf eine Organisationseinheit angewendet wurde, die sich weiter oben in der Struktur befindet, und dass es auf dieser Organisationseinheit durchgesetzt wurde, dass es dieser Organisationseinheit jedoch nicht direkt hinzugefügt wurde.

> **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 das Stammverzeichnis

Das Stammverzeichnis ist keine Organisationseinheit und kann nicht registriert oder erneut registriert werden. Sie können Konten auch nicht direkt im Stammverzeichnis erstellen. Das Stammverzeichnis darf nicht konform sein oder einen Lebenszyklusstatus haben, wie z. B. registriert oder in Drift.

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 AWS Control Tower zu integrieren, besteht darin, die Verwaltung durch AWS Control Tower auf eine gesamte Organisationseinheit (OU) auszudehnen.

Um die AWS Control Tower Tower-Governance für eine bestehende Organisationseinheit, die mit erstellt wurde AWS Organizations, und deren Konten zu aktivieren, registrieren Sie die Organisationseinheit in Ihrer AWS Control Tower Tower-Landing landing zone. Sie können Organisationseinheiten registrieren, die bis zu 300 Konten enthalten. Wenn eine Organisationseinheit mehr als 300 Konten enthält, können Sie sie nicht in AWS Control Tower registrieren.

Wenn Sie eine OU registrieren, werden ihre Mitgliedskonten in der AWS Control Tower Tower-Landing landing zone registriert. Sie unterliegen den Kontrollen, die für ihre Organisationseinheit gelten.

> **Note**
>
> Wenn Sie noch keine AWS Control Tower-Landezone haben, richten Sie zunächst eine landing zone 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 landing zone finden Sie unterErste Schritte mit AWS Control Tower.

Was passiert mit meinen Konten, wenn ich meine OU registriere?

AWS Control Tower benötigt die Genehmigung, um einen vertrauenswürdigen Zugriff zwischen AWS CloudFormation und in AWS Organizations Ihrem Namen einzurichten, AWS CloudFormation sodass Ihr Stack automatisch für die Konten in Ihrer Organisation bereitgestellt werden kann.

- Die `AWSControlTowerExecution` Rolle wird allen Konten mit dem Status Nicht registriert hinzugefügt.
- Obligatorische Kontrollen sind standardmäßig für Ihre Organisationseinheit und alle zugehörigen Konten aktiviert, wenn Sie Ihre Organisationseinheit registrieren.

Teilweise Registrierung von Konten nach der Registrierung einer Organisationseinheit

Es ist möglich, eine Organisationseinheit erfolgreich zu registrieren, bestimmte Konten können jedoch weiterhin abgemeldet werden. Falls ja, erfüllen diese Konten einige der Voraussetzungen für die Registrierung nicht. Wenn eine Kontoregistrierung im Rahmen des Prozesses „Organisationseinheit registrieren“ nicht erfolgreich ist, zeigt der Kontostatus auf der Kontoseite die Meldung Registrierung fehlgeschlagen an. 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 Organisationseinheit insgesamt 5 Konten hat und 4 davon erfolgreich registriert wurden, aber ein Konto konnte während des Prozesses „Organisationseinheit registrieren“ nicht registriert werden. Sie können die Option Organisationseinheit erneut registrieren wählen, um Konten zur Registrierung hinzuzufügen, nachdem Sie sichergestellt haben, dass die Konten die Registrierungsvoraussetzungen erfüllen.

IAM-Benutzervoraussetzungen für die Registrierung einer Organisationseinheit

Ihre AWS Identity and Access Management (IAM-) Identität (Benutzer oder Rolle) oder IAM Identity Center-Benutzeridentität muss im entsprechenden Account Factory Factory-Portfolio enthalten sein, wenn Sie den Vorgang „Organisationseinheit registrieren“ ausführen, auch wenn Sie bereits über die entsprechenden Berechtigungen verfügen`Admin`. Andernfalls schlägt die Erstellung der bereitgestellten Produkte bei der Registrierung fehl. Ein Fehler tritt auf, weil AWS Control Tower bei der Registrierung einer Organisationseinheit auf die Anmeldeinformationen des IAM-Benutzers oder der IAM Identity Center-Benutzeridentität angewiesen ist.

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 einzusehen. Weitere Informationen dazu, wie Sie Zugriff gewähren, finden Sie in der Dokumentation für. AWS Service Catalog

Registrieren Sie eine bestehende Organisationseinheit

In der AWS Control Tower-Konsole können Sie auf der Seite Organisation 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 landing zone erstellt und unterliegen keiner anderen Landezone. Sie können bestehende Organisationseinheiten registrieren, die bis zu 300 Konten enthalten. Wenn eine Organisationseinheit mehr als 300 Konten enthält, können Sie sie nicht in AWS Control Tower registrieren.

Um eine bestehende Organisationseinheit zu registrieren

1. Melden Sie sich unter https://console.aws.amazon.com/controltower bei der AWS Control Tower Tower-Konsole an.
2. Wählen Sie im linken Navigationsmenü 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 OU aufrufen können.
4. Auf der Seite mit den OU-Details können Sie oben rechts im Dropdownmenü „Aktionen“ die Option Organisationseinheit registrieren auswählen.

Der Registrierungsprozess dauert mindestens 10 Minuten, um die Verwaltung auf die Organisationseinheit auszudehnen, und bis zu 2 weitere Minuten für jedes weitere Konto.

Ergebnisse der Registrierung einer bestehenden Organisationseinheit

Nachdem Sie eine bestehende Organisationseinheit registriert haben, ermöglicht diese `AWSControlTowerExecution` Rolle AWS Control Tower, die Verwaltung auf die einzelnen Konten auszudehnen. Schutzmaßnahmen werden durchgesetzt, und Informationen über Kontoaktivitäten werden an Ihre Audit- und Logging-Konten gemeldet.

Zu den weiteren Ergebnissen gehören die folgenden:

- `AWSControlTowerExecution` ermöglicht die Prüfung durch das Prüfungskonto von AWS Control Tower.
- `AWSControlTowerExecution`hilft Ihnen, 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-Kontrollen automatisch für jedes einzelne Konto in Ihren Organisationseinheiten sowie für jedes neue Konto gelten, das Sie in AWS Control Tower erstellen.

Für eine registrierte Organisationseinheit können Sie Compliance- und Sicherheitsberichte bereitstellen, die auf den Prüf- und Protokollierungsfunktionen von AWS Control Tower Controls 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 AWS Control Tower Organisationseinheiten 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 verschieben, können Sie auf Ihrer OU-Detailseite das Ergebnis „1 von 0“ -Konten sehen. AWS Organizations Darüber hinaus haben Sie möglicherweise in dieser nicht registrierten Organisationseinheit ein weiteres Konto erstellt, für das die Registrierung aufgehoben wurde. Wenn es ein nicht registriertes Konto gibt, wird auf der Konsole möglicherweise „1 von 1“ für die Organisationseinheit angezeigt. Es

scheint, dass das einzelne (neu erstellte) Konto registriert ist, ist es aber nicht. Sie müssen das neue Konto registrieren.

Erstellen Sie eine neue Organisationseinheit

So erstellen Sie eine neue Organisationseinheit in AWS Control Tower

1. Navigieren Sie zur Seite Organisation.
2. Wählen Sie im Dropdownmenü Ressourcen erstellen oben rechts die Option Organisationseinheit erstellen aus.
3. Geben Sie im Feld OU-Name einen Namen an.
4. In der Dropdownliste „Übergeordnete Organisationseinheit“ sehen Sie die Hierarchie der registrierten Organisationseinheiten. 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 OU aus, der in der Tabelle auf der Seite Organisation angezeigt wird, sehen Sie sich die Seite mit der Organisationseinheit für diese übergeordnete Organisationseinheit an und wählen Sie dann im Dropdownmenü Aktionen oben rechts die Option OU hinzufügen aus. Die neue Organisationseinheit wird automatisch als verschachtelte Organisationseinheit unter der ausgewählten Organisationseinheit erstellt.

> **Note**
>
> Wenn deine landing zone nicht auf dem neuesten Stand ist, siehst du im Drop-down-Menü eine flache Liste statt einer Hierarchie. Selbst wenn Ihre landing zone verschachtelte Organisationseinheiten enthält, werden Sie keine L5-Organisationseinheiten in der Dropdownliste sehen, da Sie keine neue Organisationseinheit unter einer L5-Organisationseinheit erstellen können. Weitere Informationen zu verschachtelten

Organisationseinheiten in AWS Control Tower finden Sie unterVerschachtelte Organisationseinheiten im AWS Control Tower.

Häufige Ursachen für Fehler bei der Registrierung oder Neuregistrierung

Wenn die Registrierung (oder Neuregistrierung) einer Organisationseinheit oder eines ihrer Mitgliedskonten fehlschlägt, können Sie eine Datei herunterladen, die einen detaillierten Bericht enthält, aus dem hervorgeht, welche Vorabprüfungen nicht bestanden wurden. Sie können den Download abschließen, indem Sie auf die Download-Schaltfläche 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 diese Fehler korrigieren können.

Wenn Sie eine OU registrieren oder erneut registrieren, werden im Allgemeinen alle Konten innerhalb dieser OU in AWS Control Tower registriert. Es ist jedoch möglich, dass einige Konten nicht registriert werden können, selbst wenn die Organisationseinheit als Ganzes 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.

Fehler in der Landezone

- Die Landezone ist nicht bereit

  Setze deine aktuelle landing zone 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 5 SCPs pro OU gilt für alle OUs in Ihrer AWS Control Tower 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, wodurch AWS Control Tower das Konto nicht registrieren kann. Überprüfen Sie die angewendeten

SCPs auf Richtlinien, die verhindern könnten, dass AWS Control Tower funktioniert. Achten Sie darauf, die SCPs zu überprüfen, die von Organisationseinheiten übernommen wurden, die weiter oben in der Hierarchie stehen.

- Überschreitet das im Stack festgelegte

  Das Stack-Set-Kontingent wurde möglicherweise überschritten. Wenn Sie mehr Instances 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 Organisationseinheit bei der Registrierung auf 300 Konten.

Fehler beim Konto

- Vorabprüfungen von Konten wurden verhindert

  Ein vorhandenes SCP auf der Organisationseinheit verhindert, dass AWS Control Tower Vorabprüfungen Ihrer OU-Mitgliedskonten durchführt. Um diesen Fehler bei der Vorabprüfung zu beheben, aktualisieren oder entfernen Sie den SCP aus der Organisationseinheit.

- Fehler bei 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 Delivery Channel aktiviert

  Das Konto verfügt möglicherweise über einen vorhandenen AWS Config Konfigurationsrekorder oder einen Bereitstellungskanal. Diese müssen AWS CLI in allen AWS Regionen, in denen das AWS Control Tower Tower-Verwaltungskonto Ressourcen verwaltet hat, 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 von AWS Control Tower unterstützten Regionen aktiviert sein.

- Konflikt mit dem IAM Identity Center

Die AWS Control Tower Tower-Heimatregion ist nicht identisch mit der Region AWS IAM Identity Center (IAM Identity Center). Wenn IAM Identity Center bereits eingerichtet ist, muss die AWS Control Tower 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 Organisationseinheit, und versuchen Sie es erneut.

- Der IAM-Benutzer ist 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 bezieht sich nur auf das Verwaltungskonto.

- Das Konto erfüllt die Voraussetzungen nicht

  Das Konto erfüllt nicht die Voraussetzungen für die Kontoregistrierung. Beispielsweise fehlen dem Konto möglicherweise Rollen und Berechtigungen, die für die Registrierung bei AWS Control Tower erforderlich sind. Anweisungen zum Hinzufügen einer Rolle finden Sie inFügen Sie die erforderliche IAM-Rolle manuell zu einer vorhandenen hinzu AWS-Konto und registrieren Sie sie.

Zur Erinnerung: AWS CloudTrail Wird für all Ihre AWS Konten automatisch aktiviert, wenn Sie sie bei AWS Control Tower registrieren. Wenn CloudTrail es für ein Konto vor der Registrierung aktiviert ist, kann es zu Doppelabrechnungen kommen, sofern Sie es nicht deaktivieren, CloudTrail bevor Sie mit dem Registrierungsprozess beginnen.

Organisationen aktualisieren

Die schnellste Möglichkeit, eine Organisationseinheit (OU) oder mehrere Konten innerhalb einer OU zu aktualisieren, besteht darin, die OU erneut zu registrieren.

Wann sollten AWS Control Tower-OUs und -Konten aktualisiert werden

Wenn Sie eine Landing Zone-Aktualisierung durchführen, müssen Sie Ihre registrierten Konten aktualisieren, um neue Kontrollen auf diese Konten anzuwenden.

- Sie können eine Aktualisierung aller Konten unter einer Organisationseinheit mit der Option Neu registrieren durchführen.
- Wenn Sie mehr als eine registrierte Organisationseinheit in Ihrer Landing Zone haben, registrieren Sie alle Ihre OUs erneut, um alle Ihre Konten zu aktualisieren.
- Um ein einzelnes Konto zu aktualisieren, können Sie über die AWS Control Tower-Konsole aktualisieren oder die Option Bereitgestelltes Produkt aktualisieren in auswählen AWS Service Catalog. Siehe Aktualisieren Sie das Konto in der Konsole.

Aktualisieren mehrerer Konten in derselben Organisationseinheit

So aktualisieren Sie mehrere Konten in einer Organisationseinheit mit einer Aktion

1. Melden Sie sich bei der AWS Control Tower-Konsole unter https://console.aws.amazon.com/controltower an.
2. Wählen Sie im linken Navigationsmenü Organisation aus.
3. Wählen Sie auf der Seite Organisation eine beliebige Organisationseinheit aus, um die Seite mit den Organisationseinheitsdetails anzuzeigen.
4. Wählen Sie unter Aktionen oben rechts die Option Organisationseinheit erneut registrieren aus.

Wiederholen Sie diese Schritte für jede Organisationseinheit in Ihrer AWS Control Tower-Organisation, wenn Sie alle Ihre Konten und OUs aktualisieren müssen.

Alternativ können Sie ein beliebiges Konto auswählen, das den Status Update verfügbar anzeigt, und dann Konto für so viele Konten wie nötig aktualisieren auswählen.

Was passiert während der Neuregistrierung?

Wenn Sie eine Organisationseinheit erneut registrieren:

- Das Feld Status gibt an, ob das Konto derzeit bei AWS Control Tower registriert ist (Registriert), ob das Konto noch nie registriert wurde (Nicht registriert) oder ob die Registrierung zuvor fehlgeschlagen ist (Registrierung fehlgeschlagen).

- Wenn Sie die Organisationseinheit erneut registrieren, wird die `AWSControlTowerExecution` Rolle allen Konten mit dem Status Nicht registriert oder Registrierung fehlgeschlagen hinzugefügt.
- AWS Control Tower erstellt eine Single Sign-On-Anmeldung (IAM Identity Center) für diese neuen registrierten Konten.
- Registrierte Konten werden erneut bei AWS Control Tower registriert.
- Die Abweichung bei allen präventiven Kontrollen, die auf die Organisationseinheit angewendet werden, ist behoben, da die SCPs auf ihre Standarddefinitionen zurückgesetzt werden.
- Alle Konten werden aktualisiert, um die neuesten Änderungen der Landing Zone widerzuspiegeln.

Weitere Informationen finden Sie unter Registriere ein vorhandenes AWS-Konto.

> **Tip**
>
> Wenn Sie eine Organisationseinheit erneut registrieren oder Ihre Landing-Zone-Version und mehrere Mitgliedskonten aktualisieren, wird möglicherweise eine Fehlermeldung mit dem Hinweis StackSet–AWSControlTowerExecutionRole angezeigt. Dies StackSet im Verwaltungskonto kann fehlschlagen, da die AWSControlTowerExecution IAM-Rolle bereits in allen registrierten Mitgliedskonten vorhanden ist. Diese Fehlermeldung ist das erwartete Verhalten und kann ignoriert werden.

Aktualisieren eines einzelnen Kontos

Sie können einzelne AWS Control Tower-Konten in der AWS Control Tower-Konsole oder in der Service Catalog-Konsole aktualisieren.

Informationen zum Aktualisieren eines einzelnen Kontos in der AWS Control Tower-Konsole finden Sie unter Aktualisieren Sie das Konto in der Konsole.

So aktualisieren Sie ein einzelnes Konto in AWS Service Catalog

1. Wechseln Sie zu AWS Service Catalog.
2. Wählen Sie im linken Navigationsmenü 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 die Dropdownliste Aktionen unter Aktualisieren aus.

Weitere Informationen zum Aktualisieren von in AWS Service Catalogfinden Sie unter Aktualisieren Sie das bereitgestellte Produkt und Aktualisieren von Produkten im Service-Catalog-Administratorhandbuch.

Integrierte Services

AWS Control Tower ist ein Service, der auf anderen AWS Services aufbaut und Sie bei der Einrichtung einer gut strukturierten Umgebung unterstützt. Dieses Kapitel bietet einen kurzen Überblick über diese Services, einschließlich Konfigurationsinformationen über die zugrunde liegenden Services und deren Funktionsweise in AWS Control Tower.

Weitere Informationen zur Messung einer gut strukturierten Umgebung finden Sie im Well-Architected Tool AWS . Weitere Informationen finden Sie im Leitfaden zur Cloud-Umgebung für Management und Governance.

Themen

- Stellen Sie Umgebungen bereit mit AWS 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
- Serverlose Rechenfunktionen mit Lambda ausführen
- Konten verwalten über AWS Organizations
- Objekte mit Amazon S3 speichern
- Überwachen Sie Ihre Umgebung mit Security Hub
- Stellen Sie Konten bereit über AWS Service Catalog
- Verfolgen Sie Benachrichtigungen über Amazon Simple Notification Service
- Erstellen Sie verteilte Anwendungen mit AWS Step Functions

Stellen Sie Umgebungen bereit mit AWS CloudFormation

AWS 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 AWS CloudFormation ermöglicht es Ihnen, mithilfe einer Vorlagendatei eine

Sammlung von Ressourcen zu einer einzigen Einheit (einem Stapel) zu erstellen und zu löschen. Weitere Informationen finden Sie im AWS CloudFormation -Benutzerhandbuch.

AWS Control Tower verwendet AWS CloudFormation Stacksets, um Kontrollen auf Konten anzuwenden. Weitere Informationen zur Zusammenarbeit mit AWS Control Tower finden Sie unterAWS Control Tower Ressourcen erstellen mit AWS CloudFormation. AWS CloudFormation

Überwachen Sie Ereignisse mit CloudTrail

AWS Control Tower ist so konfiguriert AWS CloudTrail , dass eine zentrale Protokollierung und Prüfung möglich ist. Mit kann CloudTrail das Verwaltungskonto administrative Aktionen und Lebenszyklusereignisse für Mitgliedskonten überprüfen.

CloudTrail hilft Ihnen dabei, Ihre AWS Umgebung in der Cloud zu überwachen, indem es einen Verlauf 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 kontrollieren, 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 einsetzen können. Sie müssen nicht länger eigene Überwachungssysteme und -infrastrukturen einrichten, verwalten und skalieren. Weitere Informationen finden Sie im CloudWatch Amazon-Benutzerhandbuch.

Weitere Informationen zur Zusammenarbeit von Amazon CloudWatch mit AWS Control Tower finden Sie unter Überwachung.

Steuern Sie Ressourcenkonfigurationen mit AWS Config

AWS Config bietet eine detaillierte Ansicht der mit Ihrem AWS Konto verknüpften Ressourcen, einschließlich deren Konfiguration, ihrer Beziehung zueinander und der Art und Weise, wie sich die Konfigurationen und ihre Beziehungen im Laufe der Zeit geändert haben. Weitere Informationen finden Sie im AWS Config -Entwicklerhandbuch.

AWS Config Ressourcen, die von AWS Control Tower bereitgestellt werden, werden automatisch mit einem Tag gekennzeichnet `aws-control-tower` und haben den Wert. `managed-by-control-tower`

Weitere Informationen darüber, wie Ressourcen in AWS Control Tower AWS Config überwacht und aufgezeichnet werden und wie Ihnen diese in Rechnung gestellt werden, finden Sie unterÜberwachen von Ressourcenänderungen mit AWS Config.

AWS Control Tower wird verwendet AWS-Config-Regeln , um detektive Kontrollen zu implementieren. Weitere Informationen finden Sie unter Über Kontrollen in AWS Control Tower.

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, Sicherheitsanmeldeinformationen — wie Zugriffsschlüssel und Berechtigungen — zentral verwalten, die festlegen, auf welche AWS Ressourcen Ihre Benutzer und Anwendungen Zugriff haben.

Wenn Sie Ihre landing zone einrichten, können AWS IAM Identity Center automatisch eine Reihe von Gruppen 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 Zugriff auf das IAM Identity Center und die Benutzerberechtigungen für all Ihre AWS Konten in 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 beauftragen, 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 Developer Guide.

Informationen zur Einrichtung von AWS KMS Schlüsseln mit AWS Control Tower finden Sie unter Optionales Konfigurieren von AWS KMS Schlüsseln.

Serverlose Rechenfunktionen mit Lambda ausführen

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 zusätzlichen Verwaltungsaufwand. 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 Tower-Auditkonto programmgesteuert übernommen werden, sodass Sie andere Konten mit Lambda überprüfen können. Außerdem können Sie AWS Control Tower Lifecycle-Ereignisse verwenden, um Lambda-Funktionen auszulösen.

Konten verwalten über AWS Organizations

AWS Organizations ist ein Kontoverwaltungsdienst, mit dem Sie mehrere AWS Konten zu einer Organisation zusammenfassen können, die Sie erstellen und zentral verwalten. Mit Organizations 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, den Zugriff, die Einhaltung von Vorschriften und die 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 Organizations 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 Organisationseinheit wird erstellt, wenn Sie Ihre landing zone einrichten. Sie und andere untergeordnete Organisationseinheiten 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 zusätzliche Organisationseinheiten in Ihrer landing zone über die AWS Control Tower Tower-Konsole auf der Seite Organisationseinheiten hinzufügen.

Überlegungen

Mit AWS Control Tower erstellte Organisationseinheiten können mit Kontrollen versehen werden. OUs, die außerhalb von AWS Control Tower erstellt wurden, können standardmäßig nicht. Sie können solche Organisationseinheiten jedoch registrieren. Sobald Sie eine Organisationseinheit registriert haben, können Sie Kontrollen auf sie und ihre Konten anwenden. Informationen zur Registrierung einer Organisationseinheit finden Sie unter Registrieren einer vorhandenen Organisationseinheit bei AWS Control Tower.

Objekte mit Amazon S3 speichern

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 Management Console 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 S3-Bucket erstellt, der alle Protokolle aller Konten in Ihrer landing zone enthält.

Überwachen Sie Ihre Umgebung mit Security Hub

AWS Control Tower ist mithilfe des AWS Security Hub-Standards Service-Managed Standard: AWS Control Tower in Security Hub integriert. Weitere Informationen finden Sie unter Security Hub Hub-Standard.

Stellen Sie Konten bereit über AWS Service Catalog

AWS Service Catalog ermöglicht es IT-Administratoren, Portfolios mit zugelassenen Produkten zu erstellen, zu verwalten und an Endbenutzer zu verteilen, die dann über ein personalisiertes Portal auf die Produkte zugreifen können, die sie benötigen. 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 organisatorischer Geschäftsstandards 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.

AWS Control Tower kann auch die Service Catalog-APIs verwenden, um die Kontobereitstellung und -aktualisierung weiter zu automatisieren. Einzelheiten finden Sie im AWS Service Catalog Entwicklerhandbuch.

Übergang zum AWS Service Catalog externen Produkttyp

AWS Service Catalog Die Unterstützung für Terraform Open Source-Produkte und bereitgestellte Produkte wurde auf einen neuen Produkttyp namens External umgestellt. 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 Tower-Kontos erstellt oder registriert haben. Um diese Konten auf den Produkttyp External 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 AWS Service Catalog , sodass sie sowohl externe als auch Terraform Open Source-Produkttypen unterstützt. Anweisungen zur Aktualisierung Ihrer Terraform Reference Engine finden Sie im Repository.AWS Service Catalog GitHub

2. AWS Service CatalogDuplizieren Sie darin 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 in 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 Hinzufügen eines Blueprints zu einem AWS Control Tower Tower-Konto.
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 sie.
5. Künftig müssen alle Konten, die mit der werkseitigen Anpassung des AWS Control Tower Tower-Kontos erstellt oder registriert wurden, auf Blueprints verweisen, die den Produkttyp AWS CloudFormationoder External verwenden.

   Für Blueprints, die mit dem Produkttyp Extern 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.

> **Note**
>
> AWS Control Tower unterstützt Terraform Open Source nicht als Produkttyp bei der Erstellung neuer Konten. 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 auf diesen Produkttyp. Wenden Sie sich an Ihren Kundenbetreuer, um Unterstützung anzufordern.

Verfolgen Sie Benachrichtigungen über Amazon Simple Notification Service

Amazon Simple Notification Service (Amazon SNS) ist ein Webservice, der es Anwendungen, Endbenutzern und Geräten ermöglicht, sofort Benachrichtigungen 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 Audit-Kontos zu senden. Diese Warnmeldungen helfen Ihnen dabei, ein Driften innerhalb Ihrer landing zone 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 senden AWS Config.

> **Tip**
>
> Eine der besten Möglichkeiten, Compliance-Benachrichtigungen von AWS Control Tower Control (in Ihrem Audit-Konto) zu erhalten, ist das Abonnieren von`AggregateConfigurationNotifications`. Dieser Service hilft Ihnen dabei, die Einhaltung der Vorschriften zu überprüfen. Es gibt Ihnen echte Daten über AWS Config Regeln, die nicht mehr eingehalten werden. AWS Config verwaltet automatisch die Liste der Konten in Ihrer Organisationseinheit.
> Sie müssen das Abonnement manuell, per E-Mail oder mit einem beliebigen Abonnement, das SNS zulässt, abschließen. Die Abrechnung `arn:aws:sns:`*`homeregion`*`:`*`account`*`:aws-controltower-AggregateSecurityNotifications` führt zu Ihrem Prüfkonto.

Erstellen Sie verteilte Anwendungen mit AWS Step Functions

AWS Step Functions macht es einfach, die Komponenten verteilter Anwendungen als eine Reihe von Schritten in einem visuellen Workflow 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 in AWS Control Tower

Um jeden Vorgang in Ihrer landing zone durchzuführen, z. B. die Bereitstellung von Konten in Account Factory oder die Erstellung neuer Organisationseinheiten (OUs) in der AWS Control Tower 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 Tower-Konsole verwenden, authentifizieren Sie Ihre Identität, indem Sie Ihre von Ihrem Administrator bereitgestellten AWS Anmeldeinformationen angeben.

Nachdem Sie Ihre Identität authentifiziert haben, steuert IAM Ihren Zugriff AWS mit einem definierten Satz von Berechtigungen für eine bestimmte Gruppe von Vorgängen und Ressourcen. 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 Tower-Ressourcen
- Vermeiden Sie dienstübergreifendes Identitätsmissbrauchs
- Verwendung identitätsbasierter Richtlinien (IAM-Richtlinien) für AWS Control Tower

Authentifizierung

Sie haben Zugriff auf AWS eine der folgenden Arten von Identitäten:

- AWS Kontostammbenutzer — 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 Root-Benutzer des AWS Kontos 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 Ihren ersten IAM-Benutzer (in den meisten Anwendungsfällen keine bewährte

Methode) zu erstellen. 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 innerhalb Ihres AWS Kontos, 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 AWS Support Center anzumelden. AWS Es wird empfohlen, 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 für einen bestimmten Zweck einen IAM-Benutzer 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 Signaturprozess für Signature Version 4 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 es sich um eine AWS Identität handelt und sie 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:
  - Föderierter Benutzerzugriff — Anstatt einen IAM-Benutzer zu erstellen, können Sie vorhandene Identitäten aus AWS 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 Dienstzugriff — Eine Servicerolle ist eine IAM-Rolle, die ein Dienst übernimmt, 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 Servicerolle muss alle Berechtigungen enthalten, die der Dienst für den Zugriff auf die benötigten AWS Ressourcen benötigt. 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 für einen AWS Dienst.
- Auf Amazon EC2 ausgeführte Anwendungen — Sie können eine IAM-Rolle verwenden, um temporäre Anmeldeinformationen für Anwendungen zu verwalten, die auf einer Amazon EC2 EC2-Instance ausgeführt werden und AWS CLI- oder AWS API-Anfragen stellen. Dies ist dem Speichern von Zugriffsschlüsseln innerhalb der Amazon EC2 EC2-Instance vorzuziehen. Um einer Amazon EC2 EC2-Instance eine AWS Rolle zuzuweisen und sie allen ihren Anwendungen zur Verfügung zu stellen, erstellen Sie ein Instance-Profil, das an die Instance angehängt ist. 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 vom Benutzerportal aus 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-Zugriff 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 Konten zu ermöglichen. AWS Weitere Informationen finden Sie im AWS IAM Identity Center Benutzerhandbuch unter Berechtigungssätze.

Zugriffskontrolle

Um AWS Control Tower 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 für den Zugriff auf die entsprechenden Ressourcen. Darüber hinaus benötigen Sie gültige Zugriffsschlüssel, um die Operation programmgesteuert ausführen zu können.

In den folgenden Abschnitten wird beschrieben, wie Sie Berechtigungen für AWS Control Tower verwalten:

Themen

- Überblick über die Verwaltung von Zugriffsberechtigungen für Ihre AWS Control Tower Tower-Ressourcen
- Verwendung 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 die Verwaltung des Zugriffs auf mehrere AWS Konten und Geschäftsanwendungen. 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 zur Selbstverwaltung Ihrer Identität und Zugriffskontrolle ausgewählt.

Weitere Informationen zur Auswahl eines Identitätsanbieters finden Sie unter Anleitung 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.

Video-Walkthrough zum Einrichten AWS von IAM Identity Center in AWS Control Tower.

Informationen zum Einrichten von AWS Control Tower mit IAM Identity Center

Wenn Sie AWS Control Tower zum ersten Mal einrichten, können nur der Root-Benutzer und alle IAM-Benutzer mit den richtigen Berechtigungen IAM-Identity-Center-Benutzer hinzufügen. Nachdem

Endbenutzer jedoch der AWSAccountFactory Gruppe hinzugefügt wurden, können sie neue IAM-Identity-Center-Benutzer über den Account-Factory-Assistenten erstellen. Weitere Informationen finden Sie unter Konten mit Account Factory bereitstellen und verwalten.

Wenn Sie die empfohlene Standardeinstellung 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 kontenübergreifenden Verbundzugriff haben. Wenn Sie Ihre Landing Zone einrichten, wird dieses Standardverzeichnis so erstellt, dass es Benutzergruppen und Berechtigungssätze enthält.

> **Note**
>
> Sie können die Verwaltung von AWS IAM Identity Center in Ihrer Organisation an ein anderes Konto als das Verwaltungskonto delegieren, indem Sie die delegierte Administratorfunktion von IAM Identity Center verwenden. 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-Verwaltung.

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 eine breite Palette unterschiedlicher Benutzerberechtigungsanforderungen ab, z. B. schreibgeschützten Zugriff, administrativen Zugriff auf AWS Control Tower und Service Catalog-Zugriff. Diese Berechtigungssätze ermöglichen es Ihren Endbenutzern, schnell und in Übereinstimmung mit den Richtlinien Ihres Unternehmens ihre eigenen AWS Konten in Ihrer Landing Zone bereitzustellen.

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 Services 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 gute Dinge, die Sie bei der Arbeit mit IAM Identity Center-Benutzerkonten in AWS Control Tower beachten 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 erneut aktivieren.
- Wenn Sie beim Aktualisieren des bereitgestellten Produkts, das einem von Account Factory verkauften 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 die vorherige IAM-Identity-Center-Benutzer-E-Mail-Adresse lieber aus dem AWS IAM Identity Center entfernen möchten, finden Sie weitere Informationen unter Deaktivieren eines Benutzers.
- 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 unter Überlegungen zum Ändern 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 diese Gruppen direkt im IAM Identity Center zuweisen. Auf diese Weise werden den Benutzern in Gruppen in Ihren Konten Berechtigungssätze zugeordnet. Die folgenden Gruppen werden erstellt, wenn Sie Ihre Landing Zone einrichten.

AWSAccountFactory

Account	Berechtigungssätze	Beschreibung
Verwaltungskonto	AWSServiceCatalogEndUserAccess	Diese Gruppe wird nur in diesem Konto verwendet, um neue Konten mithilfe von Account Factory bereitzustellen.

AWSServiceCatalogAdmins

Account	Berechtigungssätze	Beschreibung
Verwaltungskonto	AWSServiceCatalogAdminFullAccess	Diese Gruppe wird nur in diesem Konto verwendet, um administrative Änderungen an Account Factory vorzunehmen. Benutzer in dieser Gruppe können keine neuen Konten bereitstellen, es sei denn, sie befinden sich ebenfalls in der AWSAccountFactory Gruppe.

AWSControlTowerAdmins

Account	Berechtigungssätze	Beschreibung
Verwaltungskonto	AWSAdministratorAccess	Benutzer dieser Gruppe in diesem Konto sind die einzigen, die Zugriff auf die AWS Control Tower-Konsole haben.
Protokollarchivkonto	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	Beschreibung
Verwaltungskonto	AWSPowerUserAccess	Benutzer können Aufgaben zur Anwendungsentwicklung ausführen und Ressourcen und Services erstellen und konfigurieren, die eine AWS -fähige Anwendungsentwickl ung unterstützen.
Protokollarchivkonto	AWSPowerUserAccess	Benutzer können Aufgaben zur Anwendungsentwicklung ausführen und Ressourcen und Services erstellen und

Account	Berechtigungssätze	Beschreibung
		konfigurieren, die eine AWS -fähige Anwendungsentwickl ung unterstützen.
Prüfungskonto	AWSPowerUserAccess	Benutzer können Aufgaben zur Anwendungsentwicklung ausführen und Ressourcen und Services erstellen und konfigurieren, die eine AWS -fähige Anwendungsentwickl ung unterstützen.
Mitgliedskonten	AWSPowerUserAccess	Benutzer können Aufgaben zur Anwendungsentwicklung ausführen und Ressourcen und Services erstellen und konfigurieren, die eine AWS -fähige Anwendungsentwickl ung unterstützen.

AWSSecurityAuditors

Account	Berechtigungssätze	Beschreibung
Verwaltungskonto	AWSReadOnlyAccess	Benutzer haben schreibge schützten Zugriff auf alle AWS Services und Ressourcen in diesem Konto.
Protokollarchivkonto	AWSReadOnlyAccess	Benutzer haben schreibge schützten Zugriff auf alle AWS Services und Ressourcen in diesem Konto.
Prüfungskonto	AWSReadOnlyAccess	Benutzer haben schreibge schützten Zugriff auf alle AWS

Account	Berechtigungssätze	Beschreibung
		Services und Ressourcen in diesem Konto.
Mitgliedskonten	AWSReadOnlyAccess	Benutzer haben schreibge schützten Zugriff auf alle AWS Services und Ressourcen in diesem Konto.

AWSLogArchiveAdmins

Account	Berechtigungssätze	Beschreibung
Protokollarchivkonto	AWSAdministratorAccess	Benutzer in diesem Konto verfügen über Administr atorzugriff.

AWSLogArchiveViewers

Account	Berechtigungssätze	Beschreibung
Protokollarchivkonto	AWSReadOnlyAccess	Benutzer haben schreibge schützten Zugriff auf alle AWS Services und Ressourcen in diesem Konto.

AWSAuditAccountAdmins

Account	Berechtigungssätze	Beschreibung
Prüfungskonto	AWSAdministratorAccess	Benutzer in diesem Konto verfügen über Administr atorzugriff.

Überblick über die Verwaltung von Zugriffsberechtigungen für Ihre AWS Control Tower Tower-Ressourcen

Jede AWS Ressource gehört einem AWS-Konto, und die Berechtigungen zum Erstellen oder Zugreifen 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 benötigen, und die spezifischen Aktionen, die für den Betrieb dieser Ressourcen zulässig sein müssen, kennen und nachverfolgen.

Themen

- Ressourcen und Betriebsabläufe von AWS Control Tower
- Über den Besitz von Ressourcen
- Zugriff auf Ressourcen verwalten
- Geben Sie die Richtlinienelemente an: Aktionen, Auswirkungen und Prinzipien
- Angeben von Bedingungen in einer Richtlinie

Ressourcen und Betriebsabläufe von AWS Control Tower

In AWS Control Tower ist die primäre Ressource eine landing zone. AWS Control Tower unterstützt auch einen zusätzlichen Ressourcentyp, Kontrollen, die manchmal auch als Guardrails bezeichnet werden. Für AWS Control Tower können Sie Kontrollen jedoch nur im Kontext einer vorhandenen landing zone verwalten. Kontrollen können als Unterressource bezeichnet werden.

Ressourcen und Unterressourcen AWS sind mit eindeutigen Amazon-Ressourcennamen (ARNs) verknüpft, wie im folgenden Beispiel gezeigt.

AWS Control Tower bietet eine Reihe von API-Vorgängen für die Arbeit mit AWS Control Tower Tower-Ressourcen. Eine Liste der verfügbaren Operationen finden Sie unter AWS Control Tower, der AWS Control Tower API-Referenz.

Weitere Informationen zu den AWS CloudFormation Ressourcen in AWS Control Tower finden Sie im AWS CloudFormation Benutzerhandbuch.

Über den Besitz von Ressourcen

Das AWS Konto besitzt die Ressourcen, die im Konto erstellt wurden, unabhängig davon, wer die Ressourcen erstellt hat. Insbesondere ist der Ressourcenbesitzer das AWS Konto der Prinzipalentität (d. h. des AWS-Konto Root-Benutzers, eines IAM Identity Center-Benutzers, eines IAM-Benutzers oder einer IAM-Rolle), das die Anfrage 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, besitzt jedoch die Landingzone-Ressource.
- Wenn Sie in Ihrem AWS Konto eine IAM-Rolle mit Berechtigungen zum Einrichten einer landing zone erstellen, kann jeder, der die Rolle übernehmen kann, eine landing zone einrichten. Ihr AWS Konto, zu dem die Rolle gehört, besitzt die landing zone Zone-Ressource.

Zugriff auf Ressourcen verwalten

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 mit einer IAM-Identität verknüpft 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

- Informationen zu identitätsbasierten Richtlinien (IAM-Richtlinien)
- Erstellen Sie Rollen und weisen Sie Berechtigungen zu
- Ressourcenbasierte Richtlinien

Informationen zu identitätsbasierten Richtlinien (IAM-Richtlinien)

Richtlinien können IAM-Identitäten angefügt werden. Sie können z. B. Folgendes tun:

- Hängen Sie eine Berechtigungsrichtlinie an einen Benutzer oder eine Gruppe in Ihrem Konto an — Um einem Benutzer Berechtigungen zur Erstellung einer AWS Control Tower Tower-Ressource zu gewähren, z. B. das Einrichten einer landing zone, können Sie eine Berechtigungsrichtlinie an einen Benutzer oder eine Gruppe anhängen, zu der der Benutzer gehört.
- 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 einem anderen Konto (AWS Konto B) kontenübergreifende Berechtigungen gewährt, oder der Administrator kann eine Rolle erstellen, die einem anderen AWS Dienst Berechtigungen 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 hinzu.
  2. Der Administrator von Konto A ordnet der Rolle eine Vertrauensrichtlinie zu. Die Richtlinie identifiziert Konto B als den Prinzipal, 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. Durch die Übernahme der Rolle können Benutzer in Konto B 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 Principal, den Sie in der Vertrauensrichtlinie angeben, um einen AWS Dienst handeln.

Erstellen Sie Rollen und weisen Sie Berechtigungen zu

Rollen und Berechtigungen ermöglichen Ihnen den Zugriff auf Ressourcen in AWS Control Tower und in anderen AWS Services, einschließlich programmatischem Zugriff 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 Anweisungen unter Erstellen einer Rolle für einen externen Identitätsanbieter (Verbund) im IAM-Benutzerhandbuch.
- IAM-Benutzer:
  - Erstellen Sie eine Rolle, die Ihr Benutzer annehmen kann. Folgen Sie den Anweisungen unter Erstellen einer Rolle für einen IAM-Benutzer 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 Tower-Landezone einrichten, benötigen Sie einen Benutzer oder eine Rolle mit der AdministratorAccessverwalteten Richtlinie. (arn:aws:iam: :aws:policy/) AdministratorAccess

Um eine Rolle für eine (IAM-Konsole) zu erstellen AWS-Service

1. Melden Sie sich bei der an AWS Management Console 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 für Service oder Anwendungsfall einen Service und dann den Anwendungsfall aus. Anwendungsfälle werden durch den Service definiert, damit die für den Service erforderliche Vertrauensrichtlinie enthalten ist.
5. Wählen Sie Weiter aus.
6. Bei Berechtigungsrichtlinien hängen die Optionen vom ausgewählten Anwendungsfall ab:

   - Wenn der Dienst die Berechtigungen für die Rolle definiert, können Sie keine Berechtigungsrichtlinien auswählen.
   - Wählen Sie aus einer begrenzten Anzahl von Berechtigungsrichtlinien aus.
   - Wählen Sie aus allen Berechtigungsrichtlinien aus.
   - Wählen Sie keine Berechtigungsrichtlinien aus, erstellen Sie die Richtlinien, nachdem die Rolle erstellt wurde, und fügen Sie die Richtlinien dann der Rolle hinzu.
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 aus, um die maximalen Rollenberechtigungen zu steuern.

      IAM enthält eine Liste der AWS verwalteten und kundenverwalteten Richtlinien in Ihrem Konto.

   b. Wählen Sie die Richtlinie aus, die für eine Berechtigungsgrenze verwendet werden soll.
8. Wählen Sie Weiter aus.
9. Die Optionen für den Rollennamen hängen vom Dienst ab:

   - Wenn der Dienst den Rollennamen definiert, können Sie den Rollennamen nicht bearbeiten.
   - Wenn der Dienst ein Präfix für den Rollennamen definiert, können Sie ein optionales Suffix eingeben.
   - Wenn der Dienst 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 können nicht von Fall zu Fall eindeutig sein.
>
> Erstellen Sie beispielsweise keine Rollen, die **`PRODROLE`** sowohl als auch benannt sind**`prodrole`**. Wenn ein Rollenname in einer Richtlinie oder als Teil eines ARN verwendet wird, unterscheidet der Rollenname zwischen Groß- und Kleinschreibung. Wenn Kunden jedoch ein Rollenname in der Konsole angezeigt wird, z. B. während des Anmeldevorgangs, wird die Groß- und Kleinschreibung nicht berücksichtigt.
> - Sie können den Namen der Rolle nicht bearbeiten, nachdem er erstellt wurde, da andere Entitäten möglicherweise auf die Rolle verweisen.

10. (Optional) Geben Sie unter Beschreibung eine Beschreibung für die 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 aus.
12. (Optional) Um die Rolle leichter zu identifizieren, zu organisieren oder nach ihr zu suchen, fügen Sie Tags als Schlüssel-Wert-Paare hinzu. Weitere Informationen zur Verwendung von Tags in IAM finden Sie unter Markieren von IAM-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 Management Console 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 Management Console, können Sie eine JSON- oder YAML-Richtlinienvorlage generieren, die Sie in AWS CloudFormation Vorlagen verwenden können.

   Wählen Sie dazu im Richtlinien-Editor Aktionen und anschließend CloudFormationVorlage generieren aus. Weitere Informationen AWS 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 Markieren von IAM-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 Management Console 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 Create Policy (Richtlinie erstellen) aus.
4. Suchen Sie im Bereich Richtlinien-Editor nach dem Abschnitt Service auswählen 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 Berechtigung außer Kraft setzen möchten, die durch eine andere Anweisung oder Richtlinie separat zulässig ist. 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 Multi-Faktor-Authentifizierungsgeräts (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 unter Aktionen, Ressourcen und Bedingungsschlüssel für AWS Dienste in der Service Authorization Reference.

   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 Qualifizierer und den Operator für die 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 miteinander verbunden 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 Management Console, können Sie eine JSON- oder YAML-Richtlinienvorlage generieren, die Sie in Vorlagen verwenden können. AWS CloudFormation

   Wählen Sie dazu im Richtlinien-Editor Aktionen und anschließend CloudFormationVorlage generieren aus. Weitere Informationen AWS 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 Markieren von IAM-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 mit AWS außerhalb des interagieren möchten. AWS Management Console Die Art und Weise, wie programmatischer 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
Mitarbeiteridentität (Benutzer, die in IAM Identity Center verwaltet werden)	Verwenden Sie temporäre 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 zu den AWS CLI finden Sie unter Konfiguration der AWS CLI zu AWS IAM Identity Center verwendenden im AWS Command Line Interface Benutzerhandbuch. • Informationen zu AWS SDKs, Tools und AWS 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 CLI, AWS SDKs oder APIs zu signieren. AWS	Folgen Sie den Anweisungen unter Verwenden temporärer Anmeldeinformationen mit AWS Ressourcen im IAM-Benutzerhandbuch.
IAM	(Nicht empfohlen) Verwenden Sie langfristige Anmeldeinformationen, um programmatische Anfragen an	Befolgen Sie die Anweisungen für die Schnittstelle, die Sie verwenden möchten.

Welcher Benutzer benötigt programmgesteuerten Zugriff?	Bis	Von
	die AWS CLI, AWS SDKs oder APIs zu signieren. AWS	• Informationen dazu finden Sie unter Authentifizierung mithilfe von IAM-Benutzeranmeldedaten im Benutzerhandbuch. AWS CLIAWS 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 Verwaltung von Zugriffsschlüsseln für IAM-Benutzer im IAM-Benutzerhandbuch.

Schützen Sie sich vor Angreifern

Weitere Informationen darüber, wie Sie sich vor Angreifern schützen können, wenn Sie anderen AWS Service Principals Berechtigungen erteilen, finden Sie unter Optionale Bedingungen für Ihre Rollenvertrauensbeziehungen. Indem Sie Ihren Richtlinien bestimmte Bedingungen hinzufügen, können Sie dazu beitragen, eine bestimmte Art von Angriff zu verhindern, der als Confused Deputy Attack bezeichnet wird. Dieser Angriff tritt auf, wenn eine Entität eine Entität mit mehr Rechten zwingt, eine Aktion auszuführen, 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. Verwendung 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.

Ressourcenbasierte 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 Tower-Konsole oder die landing zone Zone-APIs einrichten und verwalten. Um Ihre landing zone einzurichten, müssen Sie ein IAM-Benutzer mit Administratorrechten 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 Betriebsabläufe von 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 — In identitätsbasierten Richtlinien (IAM-Richtlinien) ist der Benutzer, dem die Richtlinie zugeordnet ist, der implizite Principal. 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 je nach Bedarf verwenden können. Eine vollständige Liste der AWS-weiten Schlüssel finden Sie unter Verfügbare Schlüssel für Bedingungen im IAM-Benutzerhandbuch.

Vermeiden Sie dienstübergreifendes Identitätsmissbrauchs

In der AWS Tat kann ein dienstübergreifendes Identitätswechsels zu einem Problem mit verwirrten Stellvertretern führen. Wenn ein Dienst einen anderen Dienst anruft, kommt es zu einem dienstübergreifenden Identitätswechsel, wenn ein Dienst einen anderen Dienst manipuliert, um dessen Berechtigungen zu nutzen, um auf die Ressourcen eines Kunden in einer Weise zu reagieren, die ansonsten nicht zulässig wäre. Um diesen Angriff zu verhindern, AWS bietet es Tools, die Sie beim Schutz Ihrer Daten unterstützen, sodass nur Dienste mit berechtigter Genehmigung auf Ressourcen in Ihrem Konto zugreifen können.

Wir empfehlen, die `aws:SourceAccount` Bedingungen `aws:SourceArn` und in Ihren Richtlinien zu verwenden, um die Berechtigungen zu beschränken, 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 mit dem dienstübergreifenden Zugriff verknüpft 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 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.

Verwendung 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 dadurch Berechtigungen zur Ausführung von Vorgängen auf AWS Control Tower 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 Tower-Ressourcen zur Verfügung stehen. Weitere Informationen finden Sie unter Überblick über die Verwaltung von Zugriffsberechtigungen für Ihre AWS Control Tower Tower-Ressourcen.

Für die Nutzung der AWS Control Tower Tower-Konsole sind Berechtigungen erforderlich

AWS Control Tower erstellt automatisch drei Rollen, wenn Sie eine landing zone einrichten. Alle drei Rollen sind erforderlich, um den Konsolenzugriff zu ermöglichen. AWS Control Tower teilt Berechtigungen als bewährte Methode in drei Rollen auf, um den Zugriff auf die minimalen Gruppen von Aktionen und Ressourcen zu beschränken.

Drei erforderliche Rollen

- AWS ControlTowerAdmin Rolle
- AWS ControlTowerStackSetRole
- AWS ControlTowerCloudTrailRole

Wir empfehlen Ihnen, den Zugriff auf Ihre Rollenvertrauensrichtlinien für diese Rollen einzuschränken. Weitere Informationen finden Sie unter Optionale Bedingungen für Ihre Rollenvertrauensbeziehungen.

AWS ControlTowerAdmin Rolle

Diese Rolle bietet AWS Control Tower Zugriff auf die Infrastruktur, die für die Aufrechterhaltung der landing zone von entscheidender Bedeutung ist. Die `AWS ControlTowerAdmin` Rolle erfordert eine angehängte verwaltete Richtlinie und eine Rollenvertrauensrichtlinie für die IAM-Rolle. Eine Rollenvertrauensrichtlinie ist eine ressourcenbasierte Richtlinie, die festlegt, welche Prinzipale die Rolle übernehmen können.

Hier ist ein Beispielausschnitt für diese Rollenvertrauensrichtlinie:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "controltower.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Um diese Rolle über die AWS CLI zu erstellen und sie in eine Datei mit dem Namen abzulegen`trust.json`, finden Sie hier ein Beispiel für einen CLI-Befehl:

```
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:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:DescribeAvailabilityZones",
            "Resource": "*"
        }
```

```
    ]
}
```

2. Die folgende verwaltete Richtlinie, nämlich die`AWS ControlTowerServiceRolePolicy`.

AWS ControlTowerServiceRolePolicy

Dabei AWS ControlTowerServiceRolePolicyhandelt es sich um eine AWS verwaltete Richtlinie, die Berechtigungen zur Erstellung und Verwaltung von AWS Control Tower-Ressourcen wie AWS CloudFormation Stacksets und Stack-Instances, AWS CloudTrail Protokolldateien, einem 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 `AWSControlTowerServiceRolePolicy`im AWS Managed Policy Reference Guide.

Name der verwalteten Richtlinie: `AWS ControlTowerServiceRolePolicy`

Das JSON-Artefakt für `AWS ControlTowerServiceRolePolicy` ist das Folgende:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "cloudformation:CreateStack",
                "cloudformation:CreateStackInstances",
                "cloudformation:CreateStackSet",
                "cloudformation:DeleteStack",
                "cloudformation:DeleteStackInstances",
                "cloudformation:DeleteStackSet",
                "cloudformation:DescribeStackInstance",
                "cloudformation:DescribeStacks",
                "cloudformation:DescribeStackSet",
                "cloudformation:DescribeStackSetOperation",
                "cloudformation:ListStackInstances",
                "cloudformation:UpdateStack",
                "cloudformation:UpdateStackInstances",
```

```
                "cloudformation:UpdateStackSet"
            ],
            "Resource": [
                "arn:aws:cloudformation:*:*:type/resource/AWS-IAM-Role"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "account:EnableRegion",
                "account:ListRegions",
                "account:GetRegionOptStatus"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "cloudformation:CreateStack",
                "cloudformation:CreateStackInstances",
                "cloudformation:CreateStackSet",
                "cloudformation:DeleteStack",
                "cloudformation:DeleteStackInstances",
                "cloudformation:DeleteStackSet",
                "cloudformation:DescribeStackInstance",
                "cloudformation:DescribeStacks",
                "cloudformation:DescribeStackSet",
                "cloudformation:DescribeStackSetOperation",
                "cloudformation:GetTemplate",
                "cloudformation:ListStackInstances",
                "cloudformation:UpdateStack",
                "cloudformation:UpdateStackInstances",
                "cloudformation:UpdateStackSet"
            ],
            "Resource": [
                "arn:aws:cloudformation:*:*:stack/AWSControlTower*/*",
                "arn:aws:cloudformation:*:*:stack/StackSet-AWSControlTower*/*",
                "arn:aws:cloudformation:*:*:stackset/AWSControlTower*:*",
                "arn:aws:cloudformation:*:*:stackset-target/AWSControlTower*/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
```

```
                "cloudtrail:CreateTrail",
                "cloudtrail:DeleteTrail",
                "cloudtrail:GetTrailStatus",
                "cloudtrail:StartLogging",
                "cloudtrail:StopLogging",
                "cloudtrail:UpdateTrail",
                "cloudtrail:PutEventSelectors",
                "logs:CreateLogStream",
                "logs:PutLogEvents",
                "logs:PutRetentionPolicy"
            ],
            "Resource": [
                "arn:aws:logs:*:*:log-group:aws-controltower/CloudTrailLogs:*",
                "arn:aws:cloudtrail:*:*:trail/aws-controltower*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:GetObject"
            ],
            "Resource": [
                "arn:aws:s3:::aws-controltower*/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "sts:AssumeRole"
            ],
            "Resource": [
                "arn:aws:iam::*:role/AWSControlTowerExecution",
                "arn:aws:iam::*:role/AWSControlTowerBlueprintAccess"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "cloudtrail:DescribeTrails",
                "ec2:DescribeAvailabilityZones",
                "iam:ListRoles",
                "logs:CreateLogGroup",
                "logs:DescribeLogGroups",
                "organizations:CreateAccount",
```

```
                "organizations:DescribeAccount",
                "organizations:DescribeCreateAccountStatus",
                "organizations:DescribeOrganization",
                "organizations:DescribeOrganizationalUnit",
                "organizations:DescribePolicy",
                "organizations:ListAccounts",
                "organizations:ListAccountsForParent",
                "organizations:ListAWSServiceAccessForOrganization",
                "organizations:ListChildren",
                "organizations:ListOrganizationalUnitsForParent",
                "organizations:ListParents",
                "organizations:ListPoliciesForTarget",
                "organizations:ListTargetsForPolicy",
                "organizations:ListRoots",
                "organizations:MoveAccount",
                "servicecatalog:AssociatePrincipalWithPortfolio"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:GetRole",
                "iam:GetUser",
                "iam:ListAttachedRolePolicies",
                "iam:GetRolePolicy"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:PassRole"
            ],
            "Resource": [
                "arn:aws:iam::*:role/service-role/AWSControlTowerStackSetRole",
                "arn:aws:iam::*:role/service-role/AWSControlTowerCloudTrailRole",
                "arn:aws:iam::*:role/service-role/
AWSControlTowerConfigAggregatorRoleForOrganizations"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
```

```
                "config:DeleteConfigurationAggregator",
                "config:PutConfigurationAggregator",
                "config:TagResource"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/aws-control-tower": "managed-by-control-tower"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "organizations:EnableAWSServiceAccess",
                "organizations:DisableAWSServiceAccess"
            ],
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "organizations:ServicePrincipal": [
                        "config.amazonaws.com",
                        "cloudtrail.amazonaws.com"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "iam:AWSServiceName": "cloudtrail.amazonaws.com"
                }
            }
        }
    ]
}
```

Vertrauensrichtlinie für Rollen:

```
{
    "Version": "2012-10-17",
    "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "controltower.amazonaws.com"
         ]
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Die Online-Richtlinie lautet`AWSControlTowerAdminPolicy`:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": "ec2:DescribeAvailabilityZones",
            "Resource": "*",
            "Effect": "Allow"
        }
    ]
}
```

AWS ControlTowerStackSetRole

AWS CloudFormation übernimmt diese Rolle, um Stack-Sets in Konten bereitzustellen, die von AWS Control Tower erstellt wurden. Inlinerichtlinie:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "sts:AssumeRole"
            ],
            "Resource": [
                "arn:aws:iam::*:role/AWSControlTowerExecution"
```

```
            ],
            "Effect": "Allow"
        }
    ]
}
```

Vertrauensrichtlinie

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudformation.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

AWS ControlTowerCloudTrailRole

AWS Control Tower ermöglicht dies CloudTrail als bewährte Methode und bietet diese Rolle für CloudTrail. CloudTrailübernimmt diese Rolle bei der Erstellung und Veröffentlichung von CloudTrail Protokollen. Inlinerichtlinie:

```
{
    "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

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudtrail.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

AWSControlTowerBlueprintAccess Anforderungen an die Rolle

Bei AWS Control Tower müssen Sie die `AWSControlTowerBlueprintAccess` Rolle im angegebenen Blueprint-Hub-Konto innerhalb derselben Organisation erstellen.

Name der Rolle

Der Rollenname muss lauten. `AWSControlTowerBlueprintAccess`

Vertrauensrichtlinie für Rollen

Die Rolle muss so eingerichtet sein, dass sie den folgenden Prinzipalen vertraut:

- Der Principal, der AWS Control Tower im Verwaltungskonto verwendet.
- Die `AWSControlTowerAdmin` 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 Tower-Verwaltungskontos und ersetzen Sie den Begriff *`YourControlTowerUserRole`*durch die ID der IAM-Rolle für Ihr Verwaltungskonto.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
```

```
            "Principal": {
                "AWS": [
                    "arn:aws:iam::YourManagementAccountId:role/service-role/
AWSControlTowerAdmin",

 "arn:aws:iam::YourManagementAccountId:role/YourControlTowerUserRole"
                ]
            },
            "Action": "sts:AssumeRole",
            "Condition": {}
        }
    ]
}
```

Rollenberechtigungen

Sie müssen die verwaltete Richtlinie AWSServiceCatalogAdminFullAccessan die Rolle anhängen.

AWSServiceRoleForAWSControlTower

Diese Rolle bietet AWS Control Tower Zugriff auf das Log Archive-Konto, das Audit-Konto und die Mitgliedskonten für Operationen, die für die Aufrechterhaltung der landing zone wichtig sind, wie z. B. die Benachrichtigung über verschwendete Ressourcen.

Die `AWSServiceRoleForAWSControlTower` Rolle erfordert eine angehängte verwaltete Richtlinie und eine Rollenvertrauensrichtlinie für die IAM-Rolle.

Verwaltete Richtlinie für diese Rolle: `AWSControlTowerAccountServiceRolePolicy`

Vertrauensrichtlinie für Rollen:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "controltower.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

AWSControlTowerAccountServiceRolePolicy

Diese AWS verwaltete Richtlinie ermöglicht es AWS Control Tower, in Ihrem Namen AWS Services aufzurufen, die eine automatisierte Kontokonfiguration und zentrale Verwaltung bieten.

Die Richtlinie enthält die Mindestberechtigungen für AWS Control Tower zur Implementierung der Weiterleitung von AWS Security Hub Erkenntnissen für Ressourcen, die von Security Hub-Kontrollen verwaltet werden, die Teil des Security Hub Service-Managed Standard: AWS Control Tower sind, und verhindert Änderungen, die die Verwaltung von Kundenkonten einschränken. Sie ist Teil des Prozesses zur Erkennung von AWS Security Hub Hintergrundabweichungen, der nicht direkt von einem Kunden initiiert wird.

Die Richtlinie gewährt die Erlaubnis, EventBridge Amazon-Regeln, speziell für Security Hub-Steuerungen, für jedes 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.

Dienstleiter: `controltower.amazonaws.com`

Das JSON-Artefakt für `AWSControlTowerAccountServiceRolePolicy` ist das Folgende:

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
  //For creating the managed rule
   "Sid": "AllowPutRuleOnSpecificSourcesAndDetailTypes",
   "Effect": "Allow",
   "Action": "events:PutRule",
   "Resource": "arn:aws:events:*:*:rule/*ControlTower*",
   "Condition": {
    "ForAnyValue:StringEquals": {
     "events:source": "aws.securityhub"
    },
    "Null": {
     "events:detail-type": "false"
    },
    "StringEquals": {
     "events:ManagedBy": "controltower.amazonaws.com",
     "events:detail-type": "Security Hub Findings - Imported"
    }
   }
```

```
  },
  // Other operations to manage the managed rule
  {
   "Sid": "AllowOtherOperationsOnRulesManagedByControlTower",
   "Effect": "Allow",
   "Action": [
    "events:DeleteRule",
    "events:EnableRule",
    "events:DisableRule",
    "events:PutTargets",
    "events:RemoveTargets"
   ],
   "Resource": "arn:aws:events:*:*:rule/*ControlTower*",
   "Condition": {
    "StringEquals": {
     "events:ManagedBy": "controltower.amazonaws.com"
    }
   }
  },
  // More managed rule permissions
  {
   "Sid": "AllowDescribeOperationsOnRulesManagedByControlTower",
   "Effect": "Allow",
   "Action": [
    "events:DescribeRule",
    "events:ListTargetsByRule"
   ],
   "Resource": "arn:aws:events:*:*:rule/*ControlTower*"
  },
  // Add permission to publish the security notifications to SNS
  {
   "Sid": "AllowControlTowerToPublishSecurityNotifications",
   "Effect": "Allow",
   "Action": "sns:publish",
   "Resource": "arn:aws:sns:*:*:aws-controltower-AggregateSecurityNotifications",
   "Condition": {
    "StringEquals": {
     "aws:PrincipalAccount": "${aws:ResourceAccount}"
    }
   }
  },
  // For drift verification
  {
   "Sid": "AllowActionsForSecurityHubIntegration",
```

```
    "Effect": "Allow",
    "Action": [
     "securityhub:DescribeStandardsControls",
     "securityhub:GetEnabledStandards"
    ],
    "Resource": "arn:aws:securityhub:*:*:hub/default"
   }
  ]
}
```

Aktualisierungen dieser verwalteten Richtlinie sind in der Tabelle zusammengefasst,Verwaltete Richtlinien für AWS Control Tower.

Verwaltete Richtlinien für AWS Control Tower

AWS adressiert viele gängige Anwendungsfälle durch die Bereitstellung eigenständiger IAM-Richtlinien, die von erstellt und verwaltet AWS werden. 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.

Änderung	Beschreibung	Datum
AWSControlTowerAccountServiceRolePolicy— Eine neue Richtlinie	AWS Control Tower hat eine neue servicebezogene Rolle hinzugefügt, die es AWS Control Tower ermöglicht, Ereignisregeln zu erstellen und zu verwalten und auf der Grundlage dieser Regeln die Drifterkennung für Kontrollen zu verwalten, die sich auf Security Hub beziehen. Diese Änderung ist erforderlich, damit Kunden verschobene Ressourcen in der Konsole sehen können, wenn sich diese Ressourcen auf Security	22. Mai 2023

Änderung	Beschreibung	Datum
	Hub-Steuerungen beziehen, die Teil des vom Security Hub Service verwalteten Standards sind: AWS Control Tower.	
AWS ControlTowerServiceRolePolicy – Aktualisierung auf eine bestehende Richtlinie	AWS Control Tower hat neue Berechtigungen hinzugefügt, die es AWS Control Tower ermöglichen, Aufrufe an die vom AWS Account Management Service implementierten `EnableRegion` `ListRegions` ,, und `GetRegionOptStatus` APIs zu tätigen, um das Opt-In für Kundenkonten in der landing zone (Verwaltungskonto, Protokollarchivkonto, Auditkonto, OU-Mitgliedskonten) AWS-Regionen verfügbar zu machen. Diese Änderung ist erforderlich, damit Kunden die Möglichkeit haben, die Regionsverwaltung durch AWS Control Tower auf die Opt-in-Regionen auszudehnen.	06. April 2023

Änderung	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) 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 Servicekatalog-Portfolio zu erstellen, das angeforderte Blueprint-Produkt hinzuzufügen und das Portfolio zum Zeitpunkt der Kontobereitstellung für ein angefordertes Mitgliedskonto freizugeben. Diese Änderung ist erforderlich, damit Kunden benutzerdefinierte Konten über AWS Control Tower Account Factory bereitstellen können.	28. Oktober 2022

Änderung	Beschreibung	Datum
AWS ControlTowerServiceRolePolicy – Aktualisierung auf eine bestehende Richtlinie	AWS Control Tower hat ab landing zone Version 3.0 neue Berechtigungen hinzugefügt, die es Kunden ermöglichen, AWS CloudTrail Trails auf Organisationsebene einzurichten. Für die organisationsbasierte CloudTrail Funktion müssen Kunden den vertrauenswürdigen Zugriff für den CloudTrail Service aktiviert haben, und der IAM-Benutzer oder die IAM-Rolle muss über die Berechtigung verfügen, im Verwaltungskonto einen Trail auf Organisationsebene zu erstellen.	20. Juni 2022

Änderung	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 zur Verschlüsselung ihrer CloudTrail Protokolle anzugeben. Kunden können den KMS-Schlüssel auch während der Aktualisierung oder Reparatur der landing zone ändern. Für die Aktualisierung des KMS-Schlüssels sind AWS CloudFormation Berechtigungen zum Aufrufen der AWS CloudTrail `PutEventSelector` API erforderlich. Die Änderung der Richtlinie besteht darin, der AWS ControlTowerAdminRolle das Aufrufen der AWS CloudTrail `PutEventSelector` API zu ermöglichen.	28. Juli 2021
AWS Control Tower hat begonnen, Änderungen zu verfolgen	AWS Control Tower begann, Änderungen an seinen AWS verwalteten Richtlinien nachzuverfolgen.	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 lernen auch, wie Sie andere AWS Services nutzen können, die Ihnen helfen, Ihre AWS Control Tower Tower-Ressourcen zu überwachen und zu sichern.

Datenschutz in AWS Control Tower

Das AWS Modell der mit 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. Informationen zum Datenschutz in Europa finden Sie im Blog-Beitrag AWS -Modell der geteilten Verantwortung und in der DSGVO im AWS -Sicherheitsblog.

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).
- Verwenden Sie SSL/TLS, um mit Ressourcen zu kommunizieren. AWS Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Richten Sie die API und die Protokollierung von Benutzeraktivitäten mit ein. AWS CloudTrail
- 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 140-2-validierte kryptografische Module benötigen, verwenden Sie einen FIPS-Endpunkt. Weitere Informationen über verfügbare FIPS-Endpunkte finden Sie unter Federal Information Processing Standard (FIPS) 140-2.

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 sind. 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
- Architecting for HIPAA Security and Compliance on Amazon Web Services — In diesem Whitepaper wird beschrieben, wie Unternehmen HIPAA-konforme Anwendungen erstellen AWS können.
- AWS Ressourcen zur Einhaltung von Vorschriften — Diese Sammlung von Arbeitsmappen und Leitfäden kann auf Ihre Branche und Ihren Standort zutreffen.
- AWS Config— Dieser AWS Service bewertet, wie gut Ihre Ressourcenkonfigurationen den internen Praktiken, Branchenrichtlinien und Vorschriften entsprechen.
- AWS Security Hub— 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 unterSo arbeiten AWS Regionen 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. Clients müssen außerdem Verschlüsselungssammlungen mit PFS (Perfect Forward Secrecy) wie DHE (Ephemeral Diffie-Hellman) oder ECDHE (Elliptic Curve Ephemeral Diffie-Hellman) unterstützen. 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 Walkthrough: Einrichten von Sicherheitsgruppen in 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.

Sehen Sie sich die protokollierten 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:

Themen

- Integrierte Tools für die Überwachung
- Protokollieren von AWS Control Tower-Aktionen mit AWS CloudTrail
- Lebenszyklusereignisse in AWS Control Tower
- Verwenden von 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.

Pfade auf Organisationsebene

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, wird Ihr Konto durch den AWS CloudTrail Pfad für die AWS Control Tower Tower-Organisation geregelt. 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 im Auditkonto

In AWS Control Tower haben AWS Services nur dann Zugriff auf Ihre Ressourcen, wenn die Anfrage von Ihrer Organisation oder Organisationseinheit (OU) stammt. Für alle 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 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.

Diese Richtlinie hat keinen Einfluss auf die Funktionalität Ihrer vorhandenen Workloads. Die 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
```

Weitere Informationen zu diesem Bedingungsschlüssel finden Sie in der IAM-Dokumentation und im IAM-Blogbeitrag mit dem Titel „Verwenden Sie skalierbare Kontrollen für AWS Dienste, die auf Ihre Ressourcen zugreifen“.

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 CloudWatch Events bietet einen Stream von Systemereignissen, die Änderungen an AWS Ressourcen beschreiben, nahezu in Echtzeit. CloudWatch Events 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. CloudWatchDie Funktionen von Logs ermöglichen es Ihnen, detailliertere und genauere Abfragen durchzuführen, als Sie es normalerweise tun würden. CloudTrail

Weitere Informationen finden Sie unter Protokollieren von AWS Control Tower-Aktionen mit AWS CloudTrail.

Protokollieren von AWS Control Tower-Aktionen mit AWS CloudTrail

AWS Control Tower ist in integriert, einem Service AWS CloudTrail, der die Aktionen eines Benutzers, einer Rolle oder eines - AWS Services in AWS Control Tower aufzeichnet. CloudTrail erfasst Aktionen für AWS Control Tower als Ereignisse. Wenn Sie einen Trail erstellen, können Sie die kontinuierliche Bereitstellung von CloudTrail Ereignissen an einen Amazon S3-Bucket aktivieren, einschließlich Ereignissen für AWS Control Tower.

Wenn Sie keinen Trail konfigurieren, können Sie trotzdem die neuesten Ereignisse in der CloudTrail Konsole unter Ereignisverlauf anzeigen. Anhand der von CloudTrailgesammelten Informationen können Sie die an AWS Control Tower gestellte Anfrage, die IP-Adresse, von der die Anfrage gestellt wurde, den Initiator der Anfrage, den Zeitpunkt der Anfrage und zusätzliche Details bestimmen.

Weitere Informationen zu CloudTrail, einschließlich Konfiguration und Aktivierung, finden Sie im AWS CloudTrail -Benutzerhandbuch.

AWS Control Tower-Informationen in CloudTrail

CloudTrail wird beim Erstellen des AWS Kontos in Ihrem Konto aktiviert. Wenn die unterstützte Ereignisaktivität in AWS Control Tower auftritt, wird diese Aktivität in einem - CloudTrail Ereignis zusammen mit anderen AWS -Serviceereignissen im Ereignisverlauf aufgezeichnet. Sie können

aktuelle Ereignisse in Ihrem AWS Konto anzeigen, suchen und herunterladen. Weitere Informationen finden Sie unter Anzeigen von Ereignissen mit dem CloudTrail Ereignisverlauf.

> **Note**
>
> In AWS Control Tower-Versionen vor der Landing Zone Version 3.0 hat AWS Control Tower einen Mitgliedskonto-Trail erstellt. Wenn Sie auf Version 3.0 aktualisieren, wird Ihr CloudTrail Trail aktualisiert, um ein Organisations-Trail zu werden. Bewährte Methoden beim Wechseln zwischen Trails finden Sie unter Erstellen eines organisatorischen Trails im CloudTrail - Benutzerhandbuch.

Empfohlen: Erstellen eines Trails

Erstellen Sie für eine fortlaufende Aufzeichnung der Ereignisse in Ihrem AWS Konto, einschließlich Ereignissen für AWS Control Tower, einen Trail. Ein Trail ermöglicht CloudTrail die Bereitstellung 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 stellt die Protokolldateien in dem von Ihnen angegebenen Amazon S3-Bucket bereit. Darüber hinaus können Sie andere AWS -Services konfigurieren, um die in den CloudTrail Protokollen erfassten Ereignisdaten weiter zu analysieren und entsprechend zu agieren. Weitere Informationen finden Sie hier:

- Übersicht zum Erstellen eines Trails
- Vorbereiten der Erstellung eines Trails
- Verwalten von CloudTrail Kosten
- CloudTrail Unterstützte Services und Integrationen
- Konfigurieren von Amazon SNS-Benachrichtigungen für CloudTrail
- Empfangen von CloudTrail Protokolldateien aus mehreren Regionen und Empfangen CloudTrail von Protokolldateien aus mehreren Konten

AWS Control Tower protokolliert die folgenden Aktionen als Ereignisse in CloudTrail Protokolldateien:

Öffentliche APIs

- `DisableControl`
- `EnableControl`

- GetControlOperation
- ListEnabledControls

Andere APIs

- SetupLandingZone
- UpdateAccountFactoryConfig
- ManageOrganizationalUnit
- CreateManagedAccount
- EnableGuardrail
- 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 Anforderung mit Root- oder AWS Identity and Access Management (IAM)-Benutzeranmeldeinformationen ausgeführt wurde.
- Gibt an, ob die Anforderung mit temporären Sicherheitsanmeldeinformationen für eine Rolle oder einen Verbundbenutzer gesendet wurde.
- Ob die Anforderung von einem anderen AWS Service gestellt wurde.
- Ob die Anforderung als Zugriffsverweigerung abgelehnt oder erfolgreich verarbeitet wurde.

Weitere Informationen finden Sie unter CloudTrail userIdentity-Element.

Beispiel: AWS Control Tower-Protokolldateieinträge

Ein Trail ist eine Konfiguration, die die Bereitstellung 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 Anfrage aus einer beliebigen Quelle dar und enthält Informationen über die angeforderte Aktion, das Datum und die Uhrzeit der Aktion, die Anfrageparameter usw. . CloudTrail events werden in den Protokolldateien in keiner bestimmten Reihenfolge angezeigt.

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 von Ressourcenänderungen mit AWS Config

AWS Control Tower aktiviert AWS Config für alle registrierten Konten, sodass es die Compliance durch detektivische Kontrollen überwachen, Ressourcenänderungen aufzeichnen und Ressourcenänderungsprotokolle an das Protokollarchivkonto übermitteln kann.

Wenn Ihre Landing-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 ausgeführt wird. Jede Änderung wird als Konfigurationselement (CI) modelliert, das Informationen wie die Ressourcen-ID, die Region, das Datum, an dem jede Änderung aufgezeichnet wurde, und ob sich die Änderung auf eine bekannte Ressource oder eine neu entdeckte bezieht, enthält.

Wenn Ihre Landing 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, auf Ihre Heimatregion. Kopien globaler Ressourcenänderungen werden nicht in jeder Region gespeichert. Diese Einschränkung der Ressourcenaufzeichnung entspricht AWS Config den bewährten Methoden von . Eine vollständige Liste der globalen Ressourcen finden Sie in der - AWS Config Dokumentation.

- Weitere Informationen zu AWS Configfinden Sie unter Funktionsweise AWS Config von .
- Eine Liste der Ressourcen, die unterstützen AWS Config kann, finden Sie unter Unterstützte Ressourcentypen.
- Weitere Informationen zum Anpassen der Ressourcenverfolgung in der AWS Control Tower-Umgebung finden Sie im Blogbeitrag Anpassen der AWS Config Ressourcenverfolgung in AWS Control Tower .

AWS Control Tower richtet einen AWS Config Übermittlungskanal in allen registrierten Konten ein. Über diesen Übermittlungskanal werden alle Änderungen protokolliert, die von AWS Config im Protokollarchivkonto aufgezeichnet werden, wo sie in einem Ordner in einem Amazon Simple Storage Service-Bucket gespeichert werden.

Verwalten von AWS Config Kosten in AWS Control Tower

In diesem Abschnitt wird beschrieben, wie Änderungen an Ressourcen in Ihren AWS Control Tower-Konten AWS Config aufzeichnet und Ihnen in Rechnung stellt. Diese Informationen können Ihnen helfen zu verstehen, wie Sie die mit verbundenen Kosten verwalten können AWS Config, wenn Sie AWS Control Tower verwenden. AWS Control Tower fügt keine zusätzlichen Kosten hinzu.

> **Note**
>
> Wenn Ihre Landing 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, 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 tätig ist, als Konfigurationselement (CI) aufgezeichnet wird. AWS Config berechnet Ihnen für jedes Konfigurationselement, das es generiert.

Funktionsweise AWS Config von

AWS Config zeichnet Ressourcen in jeder Region separat auf. Einige globale Ressourcen, wie 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, AWS Config generiert fünf CIs, eines für jede Region. Andere globale Ressourcen, wie z. B. von Route 53 gehostete Zonen, werden nur einmal in allen Regionen aufgezeichnet. Wenn Sie beispielsweise eine neue gehostete Route-53-Zone in einem registrierten Konto erstellen, AWS Config generiert ein CI, unabhängig davon, wie viele Regionen für dieses Konto ausgewählt sind. Eine Liste, die Ihnen hilft, diese Arten von Ressourcen zu unterscheiden, finden Sie unter Die gleiche Ressource wird mehrmals aufgezeichnet.

> **Note**
>
> Wenn AWS Control Tower mit arbeitet AWS Config, kann eine Region durch AWS Control Tower geregelt oder nicht verwaltet werden und zeichnet die Änderungen AWS Config weiterhin auf, wenn das Konto in dieser Region arbeitet.

AWS Config erkennt zwei Arten von Beziehungen in Ressourcen

AWS Config unterscheidet zwischen direkten und indirekten Beziehungen zwischen Ressourcen. Wenn eine Ressource im API-Aufruf Describe einer anderen Ressource zurückgegeben wird, werden diese Ressourcen als direkte Beziehung aufgezeichnet. Wenn Sie eine Ressource in einer direkten Beziehung zu einer anderen Ressource ändern, erstellt AWS Config kein CI für beide Ressourcen.

Wenn Sie beispielsweise eine Amazon EC2-Instance erstellen und die API eine Netzwerkschnittstelle erfordert, AWS Config betrachtet die Amazon EC2-Instance als direkte Beziehung zur Netzwerkschnittstelle. Daher AWS Config generiert 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-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 in Bezug auf eine Ressource?

Eine Liste der Ressourcenbeziehungen finden Sie in der - AWS Config Dokumentation.

Anzeigen der AWS Config Recorder-Daten für registrierte Konten

AWS Config ist in integriert, CloudWatch sodass Sie AWS Config CIs in einem Dashboard anzeigen können. Weitere Informationen finden Sie im Blogbeitrag mit dem Titel AWS Config unterstützt Amazon- CloudWatch Metriken.

Programmgesteuert können Sie Daten anzeigen AWS Config , mit der AWS CLI arbeiten oder andere AWS Tools verwenden.

Abfragen der AWS Config Recorder-Daten für eine bestimmte Ressource

Sie können die AWS CLI verwenden, um eine Liste der letzten Änderungen für eine Ressource abzurufen.

Befehl 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 von AWS Config Daten mit Amazon QuickSight

Sie können Ressourcen visualisieren und abfragen, die von AWS Config in Ihrer gesamten Organisation aufgezeichnet wurden. Weitere Informationen finden Sie unter Visualisieren von AWS Config Daten mit Amazon Athena und Amazon QuickSight.

Fehlerbehebung AWS Config in AWS Control Tower

Dieser Abschnitt enthält Informationen zu einigen Problemen, die bei der Verwendung von AWS Config mit AWS Control Tower auftreten können.

Hohe AWS Config Kosten

Wenn Ihr Workflow Prozesse umfasst, die Ressourcen häufig erstellen, aktualisieren oder löschen, oder wenn er Ressourcen in großen Zahlen verarbeitet, kann dieser Workflow eine große Anzahl von CIs generieren. Wenn Sie diese Prozesse in einem Nicht-Produktionskonto ausführen, sollten Sie erwägen, die Registrierung des Kontos aufzuheben. Möglicherweise müssen Sie den AWS Config Recorder für dieses Konto manuell deaktivieren.

> **Note**
>
> Nachdem Sie die Registrierung des Kontos aufgehoben 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 Aufheben der Verwaltung eines registrierten Kontos. Informationen zum Deaktivieren des AWS Config Recorders finden Sie unter Verwalten des Konfigurations-Recorders.

Die gleiche Ressource wird mehrmals aufgezeichnet

Überprüfen Sie, ob es sich bei der Ressource um eine globale Ressource handelt. Für Landing Zones von AWS Control Tower vor Version 3.0 AWS Config kann bestimmte globale Ressourcen einmal für jede Region aufzeichnen, in der tätig AWS Config ist. Wenn beispielsweise in acht Regionen aktiviert AWS Config ist, wird jede Rolle achtmal aufgezeichnet.

Die folgenden Ressourcen werden für jede Region, in der tätig AWS Config ist, einmal aufgezeichnet:

- `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 werden:

- `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 häufig gestellten AWS Config Fragen zu .

Lebenszyklusereignisse in AWS Control Tower

Einige von AWS Control Tower protokollierte Ereignisse sind Lebenszyklusereignisse . Der Zweck eines Lebenszyklusereignisses besteht darin, den Abschluss bestimmter AWS Control Tower-Aktionen zu markieren, die den Status von Ressourcen ändern. Lebenszyklusereignisse gelten für Ressourcen, die AWS Control Tower erstellt oder verwaltet, wie Organisationseinheiten (OUs), Konten und Kontrollen.

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 Lebenszyklusereignis automatisch als Nicht-API- AWS Serviceereignis auf. Weitere Informationen finden Sie im AWS CloudTrail -Benutzerhandbuch.
- Jedes Lebenszyklusereignis wird auch an die Amazon- EventBridge und Amazon CloudWatch -Events-Services übermittelt.

Lebenszyklusereignisse in AWS Control Tower bieten zwei Hauptvorteile:

- Da ein Lebenszyklusereignis den Abschluss einer AWS Control Tower-Aktion registriert, können Sie eine Amazon EventBridge -Regel oder eine Amazon CloudWatch Events-Regel erstellen, die die nächsten Schritte in Ihrem Automatisierungsworkflow basierend auf dem Status des Lebenszyklusereignisses 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 nutzt zur Implementierung seiner Aktionen mehrere Services. Daher wird jedes Lebenszyklusereignis erst aufgezeichnet, nachdem eine Reihe von Aktionen abgeschlossen ist. Wenn Sie beispielsweise ein Steuerelement 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 anzeigt, wann die AWS Control Tower-Aktion initiiert wurde, und einen weiteren Zeitstempel, der anzeigt, wann das Lebenszyklusereignis abgeschlossen ist, wobei Erfolg oder Fehler markiert werden.

Anzeigen von Lebenszyklusereignissen im Control Tower

Sie können Lebenszyklusereignisse auf der Seite Aktivitäten in Ihrem AWS Control Tower-Dashboard anzeigen.

- 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 Lebenszyklusereignissen in AWS Control Tower in Ihre Workflows finden Sie in diesem Blogbeitrag unter Verwenden von Lebenszyklusereignissen zur Nachverfolgung von AWS-Control-Tower-Aktionen und zum Auslösen automatisierter Workflows.

Erwartetes Verhalten von - CreateManagedAccount und UpdateManagedAccount - Lebenszyklusereignissen

Wenn Sie ein Konto erstellen oder ein Konto in AWS Control Tower registrieren, rufen diese beiden Aktionen dieselbe interne API auf. Wenn während des Prozesses ein Fehler auftritt, tritt dieser normalerweise auf, nachdem das Konto erstellt, aber nicht vollständig bereitgestellt wurde. Wenn Sie erneut versuchen, das Konto nach dem Fehler zu erstellen, oder wenn Sie versuchen, das bereitgestellte Produkt zu aktualisieren, sieht AWS Control Tower, dass das Konto bereits vorhanden ist.

Da das Konto vorhanden ist, zeichnet AWS Control Tower das `UpdateManagedAccount` Lebenszyklusereignis anstelle des `CreateManagedAccount` Lebenszyklusereignisses am Ende der Wiederholungsanforderung auf. Möglicherweise haben Sie aufgrund des Fehlers erwartet, dass ein anderes `CreateManagedAccount` Ereignis angezeigt wird. Das `UpdateManagedAccount` Lebenszyklusereignis ist jedoch das erwartete und gewünschte Verhalten.

Wenn Sie planen, Konten mithilfe automatisierter Methoden in AWS Control Tower zu erstellen oder zu registrieren, programmieren Sie die Lambda-Funktion so, dass sie nach UpdateManagedAccount Lebenszyklusereignissen sowie CreateManagedAccount Lebenszyklusereignissen sucht.

Namen des Lebenszyklusereignis

Jedes Lebenszyklusereignis ist so benannt, dass es der ursprünglichen AWS Control Tower-Aktion entspricht, die auch von AWS aufgezeichnet wird CloudTrail. Daher heißt beispielsweise ein Lebenszyklusereignis, das vom AWS Control Tower-`CreateManagedAccount` CloudTrail Ereignis stammt`CreateManagedAccount`.

Jeder Name in der nachfolgenden Liste ist ein Link zu einem Beispiel der protokollierten Details im `JSON`-Format. Die zusätzlichen Details in diesen Beispielen stammen aus den Amazon- CloudWatch 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 zum Erstellen und Bereitstellen eines neuen Kontos mithilfe der Account Factory erfolgreich abgeschlossen hat.
- `UpdateManagedAccount`: Das Protokoll zeichnet auf, ob AWS Control Tower jede Aktion erfolgreich abgeschlossen hat, um ein bereitgestelltes Produkt zu aktualisieren, das einem Konto zugeordnet ist, das Sie zuvor mithilfe der Account Factory erstellt haben.
- `EnableGuardrail`: Das Protokoll zeichnet auf, ob AWS Control Tower jede Aktion erfolgreich abgeschlossen hat, um eine Kontrolle für eine OU zu aktivieren, die von AWS Control Tower erstellt wurde.

- DisableGuardrail: Das Protokoll zeichnet auf, ob AWS Control Tower jede Aktion erfolgreich abgeschlossen hat, um eine Kontrolle für eine OU zu deaktivieren, die von AWS Control Tower erstellt wurde.
- SetupLandingZone: Das Protokoll zeichnet auf, ob AWS Control Tower jede Aktion erfolgreich abgeschlossen hat, um eine Landing Zone einzurichten.
- UpdateLandingZone: Das Protokoll zeichnet auf, ob AWS Control Tower jede Aktion zur Aktualisierung Ihrer vorhandenen Landing Zone erfolgreich abgeschlossen hat.
- RegisterOrganizationalUnit: Das Protokoll zeichnet auf, ob AWS Control Tower jede Aktion erfolgreich abgeschlossen hat, um seine Governance-Funktionen auf einer Organisationseinheit zu aktivieren.
- DeregisterOrganizationalUnit: Das Protokoll zeichnet auf, ob AWS Control Tower jede Aktion erfolgreich abgeschlossen hat, um seine Governance-Funktionen für eine Organisationseinheit zu deaktivieren.
- PrecheckOrganizationalUnit: Das Protokoll zeichnet auf, ob AWS Control Tower eine Ressource erkannt hat, die verhindern würde, dass der Vorgang „Governance erweitern“ erfolgreich abgeschlossen wird.

Die folgenden Abschnitte enthalten eine Liste der Lebenszyklusereignisse von AWS Control Tower mit Beispielen für die Details, die für jede Art von Lebenszyklusereignis protokolliert wurden.

CreateManagedAccount

Dieses Lebenszyklusereignis zeichnet auf, ob AWS Control Tower mithilfe der Account Factory erfolgreich ein neues Konto erstellt und bereitgestellt hat. Dieses Ereignis entspricht dem AWS Control Tower-`CreateManagedAccount` CloudTrail 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 erfolgreich aktualisiert hat, das einem Konto zugeordnet ist, das zuvor mithilfe der Account Factory erstellt wurde. Dieses Ereignis entspricht dem AWS Control Tower-`UpdateManagedAccount` CloudTrailEreignis. 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":"624281831893"
                    },
                "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 Kontrolle für eine OU aktiviert hat, die von AWS Control Tower verwaltet wird. Dieses Ereignis entspricht dem AWS Control Tower-`EnableGuardrail` CloudTrail Ereignis. Das Lebenszyklusereignisprotokoll enthält die `guardrailId` und `guardrailBehavior` der Kontrolle sowie die `organizationalUnitName` und `organizationalUnitId` der Organisationseinheit, für die die Kontrolle 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 Kontrolle über eine OU, die von AWS Control Tower verwaltet wird, erfolgreich deaktiviert hat. Dieses Ereignis entspricht dem AWS Control Tower-`DisableGuardrail` CloudTrail Ereignis. Das Lebenszyklus-Ereignisprotokoll enthält die `guardrailId` und `guardrailBehavior` der Kontrolle sowie die `organizationalUnitName` und `organizationalUnitId` der Organisationseinheit, für die die Kontrolle 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 AWS Control Tower erfolgreich eine Landing Zone eingerichtet hat. Dieses Ereignis entspricht dem AWS Control Tower-`SetupLandingZone` CloudTrail Ereignis. Das Lebenszyklusereignisprotokoll enthält die `rootOrganizationalId`, die ID der Organisation, die AWS Control Tower aus dem Verwaltungskonto erstellt. Der Protokolleintrag enthält auch die `organizationalUnitName` und `organizationalUnitId` für jede der OUs sowie die `accountName` und `accountId` für jedes Konto, die erstellt werden, wenn AWS Control Tower die Landing Zone 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 AWS Control Tower Ihre vorhandene Landing Zone erfolgreich aktualisiert hat. Dieses Ereignis entspricht dem AWS Control Tower-`UpdateLandingZone` CloudTrail Ereignis. Das Lebenszyklusereignisprotokoll enthält die `rootOrganizationalId`, die die ID der (aktualisierten) Organisation ist, die von AWS Control

Tower verwaltet wird. Der Protokolleintrag enthält auch die `organizationalUnitName` und `organizationalUnitId` für jede der OUs sowie die `accountName` und `accountId` für jedes Konto, die zuvor erstellt wurden, als AWS Control Tower die Landing Zone ursprünglich eingerichtet hat.

```
{
    "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 AWS Control Tower seine Governance-Funktionen erfolgreich auf einer Organisationseinheit aktiviert hat. Dieses Ereignis entspricht dem AWS Control Tower-`RegisterOrganizationalUnit` CloudTrail Ereignis. Das Lebenszyklus-Ereignisprotokoll enthält die `organizationalUnitName` und `organizationalUnitId` der Organisationseinheit, die AWS Control Tower in seine Governance aufgenommen 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 AWS Control Tower seine Governance-Funktionen auf einer Organisationseinheit erfolgreich deaktiviert hat. Dieses Ereignis entspricht dem AWS Control Tower-`DeregisterOrganizationalUnit` CloudTrail Ereignis. Das Lebenszyklusereignisprotokoll enthält die `organizationalUnitName` und `organizationalUnitId` der Organisationseinheit, für die 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 deregistered an
 organizational unit, and enabled mandatory guardrails on the new 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 Vorabprüfungen an einer Organisationseinheit erfolgreich durchgeführt hat. Dieses Ereignis entspricht dem AWS Control Tower-`PrecheckOrganizationalUnit` CloudTrail Ereignis. Das Lebenszyklusereignisprotokoll enthält ein Feld für die `failedPrechecks` Werte `IdName`, und für jede Ressource, für die AWS Control Tower während des OU-Registrierungsprozesses Vorabprüfungen durchgeführt hat.

Das Ereignisprotokoll enthält auch Informationen zu den verschachtelten Konten, für die die Vorabprüfungen durchgeführt wurden, einschließlich der `failedPrechecks` Felder `accountId`, und `accountName`.

Wenn der `failedPrechecks` Wert leer ist, bedeutet dies, dass alle Vorabprüfungen für diese Ressource erfolgreich bestanden wurden.

- Dieses Ereignis wird nur ausgegeben, wenn eine Vorprüfung fehlschlägt.
- Dieses Ereignis wird nicht ausgegeben, wenn Sie eine leere Organisationseinheit 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"
}
```

Verwenden von AWS Benutzerbenachrichtigungen mit AWS Control Tower

Sie können AWS Benutzerbenachrichtigungen verwenden, um Übermittlungskanäle einzurichten, um über AWS Control Tower Ereignisse benachrichtigt zu werden. Sie erhalten eine Benachrichtigung, wenn ein Ereignis einer von Ihnen angegebenen Regel entspricht. Sie können Benachrichtigungen für Ereignisse über mehrere Kanäle erhalten, einschließlich E-Mail, AWS Chatbot Chat-Benachrichtigungen oder Push-Benachrichtigungen der AWS Console Mobile App. Benachrichtigungen werden auch im Console Notifications Center angezeigt.

AWS User Notifications unterstützt die Aggregation, wodurch die Anzahl der Benachrichtigungen, die Sie bei bestimmten Ereignissen erhalten, reduziert werden kann. Benachrichtigungen sind auch im Console Notifications Center sichtbar.

Zu den Vorteilen des Abonnierens von Benachrichtigungen über AWS Benutzerbenachrichtigungen EventBridge gehören:

- Eine benutzerfreundlichere Benutzeroberfläche (UI).
- Integration in die AWS Konsole im Bereich Glocke/Benachrichtigungen auf der globalen Navigationsleiste.
- Native Unterstützung für E-Mail-Benachrichtigungen, Amazon SNS muss nicht eingerichtet werden.
- Insbesondere Unterstützung für mobile Push-Benachrichtigungen, mit Ausnahme von AWS Benutzerbenachrichtigungen.

Eine Art von Benachrichtigung, die Sie möglicherweise erhalten möchten, ist beispielsweise im Falle kritischer und hochgradig schwerwiegender Erkenntnisse von Security Hub. Ein Codeausschnitt in JSON zum Einrichten dieses Benachrichtigungsabonnements könnte etwa wie folgt aussehen:

```
{
  "detail": {
    "findings": {
      "Compliance": {
        "Status": ["FAILED", "WARNING", "NOT_AVAILABLE"]
      },
      "RecordState": ["ACTIVE"],
      "Severity": {
        "Label": ["CRITICAL", "HIGH"]
      },
      "Workflow": {
        "Status": ["NEW", "NOTIFIED"]
      }
    }
  }
}
```

Ereignisfilterung

- Sie können Ereignisse nach Service und Namen filtern, indem Sie die Filter verwenden, die in der Konsole für AWS Benutzerbenachrichtigungen verfügbar sind.
- Sie können Ereignisse nach bestimmten Eigenschaften filtern, wenn Sie Ihren eigenen EventBridge Filter aus dem JSON-Code erstellen.

AWS Control Tower Beispielereignis

Hier ist ein generalisiertes Beispielereignis für AWS Control Tower.

- Es handelt sich um ein EventBridge Ereignis.
- Sie können EventBridge Ereignisse (wie diese) 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 9 event names 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
        }
    }
}
```

Anleitungen

Dieses Kapitel enthält exemplarische Verfahren, die Ihnen bei der Verwendung von AWS Control Tower helfen können.

Themen

- Walkthrough: Von ALZ zu AWS Control Tower wechseln
- Walkthrough: Automatisieren der Kontobereitstellung in AWS Control Tower über Service-Catalog-APIs
- Exemplarische Vorgehensweise: Konfiguration von AWS Control Tower ohne VPC
- Verwalten von AWS Control Tower-Ressourcen
- Walkthrough: Einrichten von Sicherheitsgruppen in AWS Control Tower mit AWS Firewall Manager
- Exemplarische Vorgehensweise: Außerbetriebnahme einer AWS Control Tower Tower-Landezone

Walkthrough: Von ALZ zu AWS Control Tower wechseln

Viele AWS Kunden haben die AWS Landing Zone-Lösung (ALZ) eingeführt, um eine sichere, konforme AWS Umgebung mit mehreren Konten einzurichten. Um den Aufwand für die Verwaltung einer Landing Zone zu reduzieren, hat den verwalteten Service namens AWS Control Tower AWS erstellt.

Für ALZ sind keine zusätzlichen Funktionen geplant. Sie werden nur langfristig unterstützt. Daher empfehlen wir Ihnen, von ALZ aus zum AWS Control Tower-Service zu wechseln. Der Blog, der in diesem Kapitel verknüpft ist, führt Sie durch verschiedene Überlegungen zu diesem Schritt und erklärt, wie Sie eine erfolgreiche Migration von ALZ zu AWS Control Tower planen können.

Blog: Migration der AWS Landing Zone-Lösung zu AWS Control Tower

AWS Prescriptive Guidance bietet eine umfassendere Dokumentation, einschließlich der Schritte für den Übergang von ALZ zu 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 zu AWS Control Tower.

Walkthrough: Automatisieren der Kontobereitstellung in AWS Control Tower über Service-Catalog-APIs

AWS Control Tower ist in mehrere andere - AWS Services integriert, z. B. AWS Service Catalog. Sie können die APIs verwenden, um Ihre Mitgliedskonten in AWS Control Tower zu erstellen und bereitzustellen.

Das Video zeigt Ihnen, wie Sie Konten in automatisierter Batch- Weise 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 veranschaulicht 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 zur Automatisierung von Kontoaktualisierungen anpassen, indem Sie die `UpdateProvisionedProduct` API von AWS Service Catalog für jedes Konto aufrufen. Sie können ein Skript schreiben, um die Konten nacheinander zu aktualisieren.

Wenn Sie mit Terraform vertraut sind, können Sie als völlig andere Automatisierungsmethode Konten mit AWS Control Tower Account Factory for Terraform (AFT) bereitstellen.

Beispiel für eine Automatisierungs-Verwaltungsrolle

Hier finden Sie eine Beispielvorlage, mit der Sie Ihre Automatisierungsverwaltungsrolle im Verwaltungskonto konfigurieren können. 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 Automatisierungsausführungsrolle

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 enthalten.

Beispiel für eine Bereitstellungseingabe für die Service-Catalog-API

Hier ist ein Beispiel für die Eingabe, die Sie der Service Catalog`ProvisionProduct`-API geben können, wenn Sie die API zur Bereitstellung von AWS Control Tower-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 `OU_NAME` in geändert `ManagedOrganizationalUnit` hat`OU_NAME (OU_ID)`. Das folgende Video erwähnt diese Änderung nicht.

Video-Anleitung

In diesem Video (6:58) wird beschrieben, wie Sie Kontobereitstellungen in AWS Control Tower automatisieren. 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.

Exemplarische Vorgehensweise: Konfiguration von AWS Control Tower ohne VPC

In diesem Thema wird beschrieben, wie Sie Ihre AWS Control Tower 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 Factory-Einstellungen so ändern, dass neue AWS Control Tower Tower-Konten ohne zugehörige VPC erstellt werden.

> **Important**
>
> 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.

Löschen Sie die AWS Control Tower VPC

Außerhalb von AWS Control Tower hat jeder AWS Kunde eine Standard-VPC, die Sie auf der Amazon Virtual Private Cloud (Amazon VPC) -Konsole unter https://console.aws.amazon.com/vpc/ einsehen können. 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 Tower-Standard-VPC. Die neue VPC ist mit Ihrem AWS Control Tower Tower-Managementkonto verknüpft. In diesem Thema wird diese neue VPC als Control Tower VPC bezeichnet.

Wenn Sie Ihre AWS Control Tower VPC in der Amazon VPC-Konsole aufrufen, wird Ihnen 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 ist bereits eine AWS (Standard-) VPC für das AWS Control Tower Tower-Managementkonto vorhanden. Um die bewährten Sicherheitsmethoden zu befolgen, empfiehlt es sich, wenn Sie die AWS Control Tower Tower-VPC löschen, auch die mit dem Verwaltungskonto verknüpfte AWS Standard-VPC aus allen AWS Regionen zu löschen. Um das Verwaltungskonto zu sichern, entfernen Sie daher die Standard-VPC aus jeder Region sowie die von Control Tower in Ihrer AWS Control Tower Tower-Heimatregion erstellte VPC.

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 keine VPCs automatisch erstellt werden.

Über das AWS Control Tower Tower-Dashboard können Sie Ihre Netzwerkkonfigurationseinstellungen anzeigen und bearbeiten. Nachdem Sie die Einstellungen so geändert haben, dass AWS Control Tower Tower-Konten ohne zugeordnete 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 Tower-Konsole unter https://console.aws.amazon.com/controltower.

2. Wählen Sie Account Factory aus dem Menü auf der linken Seite.
3. Anschließend wird die Account Factory Factory-Seite mit dem Abschnitt Netzwerkkonfiguration angezeigt.
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 beiden folgen, um sicherzustellen, dass AWS Control Tower bei der Bereitstellung eines Kontos keine VPC erstellt.

   a. Option 1 — Subnetze entfernen

      - Deaktivieren Sie den Schalter für das Internet-accessible subnet (Subnetz, auf das das Internet zugreifen kann).
      - Legen Sie den Wert Maximum number of private subnets (Maximale Anzahl an privaten Subnetzen) auf 0 fest.

   b. Option 2 — Regionen entfernen AWS

      - 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 verfügt möglicherweise über Abhängigkeiten oder Ressourcen in der AWS Control Tower VPC, 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.

Walkthrough: Einrichten von Sicherheitsgruppen in AWS Control Tower mit AWS Firewall Manager

Das Video zeigt Ihnen, wie Sie den AWS Firewall Manager-Service verwenden, um Ihre Netzwerksicherheit für 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 und wie Sie nicht konforme Ressourcen durch automatische Anwendung von Richtlinien beheben können. Sie können die Sicherheitsgruppen anzeigen, 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.

Einrichten von Sicherheitsgruppen mit AWS Firewall Manager

In diesem Video (8:02) wird beschrieben, wie Sie eine bessere Netzwerkinfrastruktursicherheit für Ihre Ressourcen und Workloads in 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.

Video-Walkthrough zur Firewall-Einrichtung in AWS Control Tower.

Weitere Informationen finden Sie in der Dokumentation zur Einrichtung von AWS WAF .

Exemplarische Vorgehensweise: 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 AWS 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. AWS 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 `OrganizationsFullAccessRole` 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 `OrganizationsFullAccessRole` 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.

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 zwei Organisationseinheiten (OUs) mit den Namen Security und Sandbox ein. 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.

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`

Amazon-S3-Buckets

Während der Einrichtung erstellt AWS Control Tower Buckets im Logging-Konto für die Protokollierung und für die Protokollierung des Zugriffs. Bei der Außerbetriebnahme Ihrer Landing Zone werden die folgenden Ressourcen nicht entfernt:

- S3-Buckets für die Protokollierung und die Protokollierung von Zugriffen im Protokollierungskonto werden nicht entfernt.
- Inhalte der Buckets für die Protokollierung und die Protokollierung von Zugriffen werden nicht entfernt.

Geteilte Konten

Zwei gemeinsame Konten (Audit und Log Archive) werden während der Einrichtung von AWS Control Tower in der Security OU erstellt. Dies geschieht, wenn Sie Ihre Landing Zone außer Betrieb nehmen:

- Gemeinsame Konten, 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-MANAGEMENT` Blueprints erstellt. Diese Protokollgruppe wird nicht entfernt. Stattdessen wird die Vorlage gelöscht und die Ressourcen bleiben erhalten.

- Diese Protokollgruppe muss manuell gelöscht werden, bevor Sie eine andere Landing Zone einrichten.

> **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 gemeinsamen Konten 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 unterVerwalten von AWS Control Tower-Ressourcen.

Verwalten von AWS Control Tower-Ressourcen

Dieses Dokument enthält Anweisungen zum einzelnen Entfernen von AWS Control Tower-Ressourcen im Rahmen regelmäßiger Wartungs- und Verwaltungsaufgaben. Die in diesem Kapitel beschriebenen Verfahren dienen nur dazu, einzelne Ressourcen oder einige Ressourcen bei Bedarf zu entfernen. Es entspricht nicht der Außerbetriebnahme Ihrer Landing Zone.

Für zwei Arten von Aufgaben müssen Sie möglicherweise Ressourcen entfernen:

- Um Ressourcen zu löschen, während Sie Ihre Landing Zone in gewöhnlichen Situationen verwalten.
- So bereinigen Sie Ressourcen, die nach der automatischen Außerbetriebnahme verbleiben.

Warning

Durch das manuelle Entfernen von Ressourcen können Sie keine neue Landing Zone einrichten. Sie ist nicht dasselbe wie die Außerbetriebnahme. Wenn Sie beabsichtigen, Ihre Landing Zone von AWS Control Tower außer Betrieb zu nehmen, folgen Sie den Anweisungen unter , Exemplarische Vorgehensweise: Außerbetriebnahme einer AWS Control Tower Tower-Landezone bevor Sie die in diesem Kapitel beschriebenen Maßnahmen ergreifen. Die Anweisungen in diesem Kapitel können Ihnen helfen, Ressourcen zu bereinigen, die nach Abschluss der automatischen Außerbetriebnahme verbleiben. Auch wenn Sie alle Ihre Landing-Zone-Ressourcen manuell löschen, entspricht dies nicht der Außerbetriebnahme der Landing Zone, und es können unerwartete Gebühren anfallen.

Wenn Sie ein Konto aus AWS Control Tower entfernen müssen, lesen Sie die folgenden Abschnitte, um ein Konto zu schließen:

- Aufheben der Verwaltung eines Kontos
- Schließen eines in Account Factory erstellten Kontos

Muss ich außer Betrieb nehmen, anstatt sie zu löschen?

Wenn Sie nicht mehr beabsichtigen, AWS Control Tower für Ihr Unternehmen zu verwenden, oder wenn Sie eine größere Neubereitstellung Ihrer Organisationsressourcen benötigen, sollten Sie die bei der Ersteinrichtung Ihrer Landing Zone erstellten Ressourcen außer Betrieb nehmen.

- Nachdem der Außerbetriebnahmeprozess abgeschlossen ist, verbleiben einige Ressourcenartefakte, z. B. Amazon S3-Buckets und Amazon- CloudWatch Logs-Protokollgruppen.
- Sie müssen die verbleibenden Ressourcen in Ihren Konten manuell bereinigen, bevor Sie eine andere Landing Zone einrichten, und die Möglichkeit unerwarteter Gebühren vermeiden. Weitere Informationen finden Sie unter Ressourcen, die bei der Außerbetriebnahme nicht entfernt wurden.

> **Warning**
>
> Es wird dringend empfohlen, einen Außerbetriebnahmeprozess nur durchzuführen, wenn Sie beabsichtigen, Ihre Landing Zone nicht mehr zu verwenden. Dieser Vorgang kann nicht rückgängig gemacht werden.

Entfernen von AWS Control Tower-Ressourcen

Die einzelnen Verfahren in diesem Kapitel führen Sie durch manuelle Methoden zum Entfernen von AWS Control Tower-Ressourcen. Diese Verfahren können befolgt werden, wenn Sie eine bestimmte Ressource aus Ihrer Landing Zone löschen müssen.

Bevor Sie diese Verfahren ausführen, müssen Sie bei der AWS Management Console in der Heimatregion für Ihre Landing Zone angemeldet sein, und Sie müssen als IAM-Benutzer oder -Benutzer im IAM Identity Center mit Administratorberechtigungen für das Verwaltungskonto angemeldet sein, das Ihre Landing Zone enthält.

> **Warning**
>
> Dies sind destruktive Aktionen, die zu Governance-Abweichungen in Ihrem AWS Control Tower-Setup führen können. Sie können nicht rückgängig gemacht werden.

Themen

- SCPs löschen

- Löschen von - StackSets und -Stacks
- Löschen von Amazon S3-Buckets im Log-Archive-Konto
- Entfernen eines Account Factory-Portfolios und -Produkts
- Rollen und Richtlinien von AWS Control Tower entfernen
- AWS Control Tower-Ressourcenhilfe

SCPs löschen

AWS Control Tower verwendet Service-Kontrollrichtlinien (SCPs) für seine Kontrollen. In diesem Verfahren wird beschrieben, wie Sie die SCPs löschen, die sich speziell auf AWS Control Tower beziehen.

So löschen Sie AWS Organizations SCPs

1. Öffnen Sie die Organizations-Konsole unter https://console.aws.amazon.com/organizations/.
2. Öffnen Sie die Registerkarte Policies (Richtlinien) und suchen Sie die Service-Kontrollrichtlinien (SCP) mit dem Präfix aws-guardrails-. Führen Sie dann für jede dieser SCPs die folgenden Schritte aus:
   a. Trennen Sie die SCP von der zugewiesenen Organisationseinheit.
   b. Löschen Sie die SCP.

Löschen von - StackSets und -Stacks

AWS Control Tower verwendet - StackSets und -Stacks zur Bereitstellung im AWS-Config-Regeln Zusammenhang mit Kontrollen in Ihrer Landing Zone. Die folgenden Verfahren zeigen, wie Sie diese Ressourcen löschen.

So löschen Sie AWS CloudFormation StackSets

1. Öffnen Sie die - AWS CloudFormation Konsole unter https://console.aws.amazon.com/cloudformation.
2. Wählen Sie im linken Navigationsmenü StackSets.
3. Gehen Sie für jedes StackSet mit dem Präfix wie folgt AWSControlTowervor. Wenn Sie viele Konten in einer haben StackSet, kann dies einige Zeit dauern.

a. Wählen Sie den spezifischen StackSet aus der Tabelle im Dashboard aus. Dadurch wird die Seite „Eigenschaften“ für diese geöffnet StackSet.

b. Machen Sie unten auf der Seite in der Tabelle Stacks einen Datensatz der AWS Konto-IDs für alle Konten in der Tabelle. Kopieren Sie die Liste mit allen Konten.

c. Wählen Sie unter Aktionen die Option Stacks löschen aus StackSet.

d. Wählen Sie unter Bereitstellungsoptionen festlegen unter Bereitstellungsspeicherorte die Option Stacks in Konten bereitstellen aus.

e. Geben Sie im Textfeld die AWS Konto-IDs ein, für die Sie in Schritt 3.b einen Datensatz erstellt haben, getrennt durch Kommas. 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 Seite StackSet Eigenschaften können Sie dieses Verfahren für Ihre anderen erneut starten 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 Tabelle Stacks leer sind, wählen Sie Löschen aus StackSet.

So löschen Sie AWS CloudFormation Stacks

1. Öffnen Sie die - AWS CloudFormation Konsole unter https://console.aws.amazon.com/cloudformation.

2. Suchen Sie im Stacks-Dashboard nach allen Stacks mit dem Präfix AWSControlTower.

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 von Amazon S3-Buckets im Log-Archive-Konto

Die folgenden Verfahren führen Sie durch die Anmeldung beim Protokollarchivkonto als IAM-Identity-Center-Benutzer in der AWSControlTowerExecution Gruppe und löschen dann die Amazon S3-Buckets in Ihrem Protokollarchivkonto.

So melden Sie sich mit den richtigen Berechtigungen bei Ihrem Protokollarchivkonto an

1. Öffnen Sie die Organizations-Konsole 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 einAWSControlTowerExecution.
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-Buckets

1. Öffnen Sie die Amazon-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.

Entfernen eines Account Factory-Portfolios und -Produkts

Das folgende Verfahren führt Sie durch die Vorgehensweise, wie Sie sich als IAM-Identity-Center-Benutzer bei der -AWSServiceCatalogAdminsGruppe anmelden und dann Ihr Account-Factory-Portfolio und Ihre Produkte bereinigen.

So melden Sie sich mit den richtigen Berechtigungen bei Ihrem Verwaltungskonto an

1. Rufen Sie Ihre Benutzerportal-URL unter *`directory-id`*.awsapps.com/start auf.
2. Suchen Sie unter AWS Konto das Verwaltungskonto.
3. Wählen Sie unter die Option -Managementkonsole ausAWSServiceCatalogAdminFullAccess, um sich AWS Management Console als diese Rolle bei der anzumelden.

So bereinigen Sie die Account Factory

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 der Seite und wählen Sie das Optionsfeld für die Einschränkung mit dem Produktnamen AWS Control Tower Account Factory aus.
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 Abschnitt Produkte der Seite das Optionsfeld für das Produkt mit dem Namen 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 Seite Admin-Produkte nach dem Produkt namens 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.

So löschen Sie die IAM-Identity-Center- AWSServiceCatalogEndUserAccess Rolle

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, bei der es sich um die Region handelt, in der Sie AWS Control Tower ursprünglich eingerichtet haben.
3. Wählen Sie im linken Navigationsmenü AWS Konten aus.
4. Wählen Sie den Link für Ihr Verwaltungskonto aus.
5. Wählen Sie das Dropdown-Menü für Berechtigungssätze aus, wählen Sie aus AWSServiceCatalogEndUserAccessund 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 sie aus AWSServiceCatalogEndUserAccess und löschen Sie sie.

So löschen Sie IAM-Rollen

1. Öffnen Sie die IAM-Konsole unter https://console.aws.amazon.com/iam/.
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.

So löschen Sie IAM-Richtlinien

1. Öffnen Sie die IAM-Konsole unter https://console.aws.amazon.com/iam/.
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.

AWS Control Tower-Ressourcenhilfe

Wenn beim Entfernen von AWS Control Tower-Ressourcen Probleme auftreten, die Sie nicht beheben können, wenden Sie sich an den AWS Support .

Wie man eine landing zone außer Betrieb nimmt

Gehen Sie wie hier beschrieben vor, um Ihre AWS Control Tower Tower-Landezone außer Betrieb zu nehmen.

> **Note**
>
> Wir empfehlen Ihnen, die Verwaltung Ihrer registrierten Konten vor der Außerbetriebnahme aufzuheben.

1. Navigieren Sie in der AWS Control Tower Tower-Konsole zur Seite Landing Zone Settings.
2. Wählen Sie im Abschnitt landing zone stilllegen die Option landing zone außer Betrieb setzen.
3. 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.

4. 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.
5. 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 Entfernen von AWS Control Tower-Ressourcen.
6. 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
```

Nach der Außerbetriebnahme sind manuelle Bereinigungsaufgaben erforderlich

- 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 zuerst 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 CloudFormation AWS-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.

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 wieder eine landing zone aufrufen, 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 Mitnahme 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 verwaltete Regel (genanntAWSControlTowerManagedRule) aus den gemeinsamen Konten und Mitgliedskonten aller verwalteten Regionen.

> **Note**
>
> Sie können in einer Organisation mit Organisationseinheiten der obersten Ebene, die entweder Security oder Sandbox heißen, keine neue landing zone einrichten. Sie müssen diese OUs umbenennen oder entfernen, um erneut eine Landing Zone einrichten zu können.

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.

Start der Landing Zone fehlgeschlagen

Häufige Ursachen für Fehler beim Starten der Landing Zone:

- Fehlende Antwort auf eine Bestätigungs-E-Mail-Nachricht.
- AWS 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 AWS CloudFormation StackSet Ausfall. 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.

Eine Liste der von AWS-Regionen AWS Control Tower unterstützten Programme finden Sie unterSo arbeiten AWS Regionen mit AWS Control Tower.

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 für den Zugriff auf AWS Control Tower aktualisieren.

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 Konten mit AWS Service Catalog Account Factory bereitstellen .

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 AWS 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.
- Kontext/Auswirkung: Die bereitgestellten AWS Konfigurationsregeln entsprechen nicht der Konfiguration, 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.

- Kontext/Auswirkung: 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, die mit der vorherigen Organisationseinheit verknüpft waren, nicht gelöscht werden.

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: 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 in der AWS Config Dokumentation

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

Fehler: Keine Startpfade gefunden

Wenn Sie versuchen, ein neues Konto zu erstellen, wird möglicherweise eine Fehlermeldung ähnlich dieser angezeigt:

```
No launch paths found for resource: prod-dpqqfywxxxx
```

Diese Fehlermeldung wird von generiert AWS Service Catalog, dem integrierten Service, der bei der Bereitstellung von Konten in AWS Control Tower hilft.

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 AWS Control Tower-OUs und -Konten 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 von der AWS Organizations API zurückgegeben

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 removing-and-deleting muss für jede verbleibende Ressource, 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.

Bei der Einrichtung der landing zone kann es sich bei dem Basisziel um ein gemeinsames Konto oder um die gesamte landing zone handeln. Bestimmte Baselines können auf der Grundlage Ihrer Landezoneneinstellungen und -konfigurationen aktiviert und aktualisiert werden. AWS Control Tower erstellt die Ressourcen und stellt sie auf dem Ziel bereit, wie es die Baseline vorgibt.

Wenn Sie eine Baseline für ein Ziel aktivieren, wird die Baseline als Ressource dargestellt, die als AWS CloudFormation Ressource bezeichnet wird. `EnabledBaseline`

AWS Control Tower umfasst vier grundlegende Arten von Baselines:

- Ein Typ kann für eine OU gelten, die bei AWS Control Tower registriert ist, oder für eine OU, die Sie registrieren möchten, indem Sie die Baseline anwenden.
- Drei Basisarten können für eine landing zone oder ein geteiltes Konto, bei der Ersteinrichtung oder während eines Landingzone-Updates gelten.

Baseline-Typ, der auf OU-Ebene für die Registrierung und Aktualisierung von Organisationseinheiten gilt

- Name (Name: `AWSControlTowerBaseline`

  Beschreibung: Richtet Ressourcen und obligatorische Kontrollen für Mitgliedskonten innerhalb der Ziel-OU ein, die für die AWS Control Tower Tower-Governance erforderlich sind.

  Überlegung: Diese Basislinie behält die Einstellungen der landing zone Region Deny Control bei. Mit anderen Worten, wenn eine Region auf Landingzone-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 Option Region Deny Control auf OU-Ebene hat keine Möglichkeit, Regionen zuzulassen, die die landing zone Region Deny Control nicht zulässt.

Weitere Informationen finden Sie in der Dokumentation unter So arbeiten SCPs mit Deny. AWS Organizations

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.

> **Note**
>
> Landingzone-Baselines verhalten sich anders als Baselines auf OU-Ebene.

AWS Control Tower aktiviert die Baselines, die auf der Ebene der landing zone gelten, automatisch als Teil des Einrichtungs- und Aktualisierungsprozesses für die landing zone. 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.

Basisarten, die für deine landing zone oder deine geteilten Konten gelten können

- Name (Name: `AuditBaseline`

  Beschreibung: Richtet Ressourcen ein, um die Sicherheit und Einhaltung der Vorschriften für Konten in Ihrer Organisation zu überwachen. Sie können diese Baseline nicht ändern, sie wird von AWS Control Tower bereitgestellt.
- Name (Name: `LogArchiveBaseline`

Beschreibung: Richtet ein zentrales Repository für Protokolle von API-Aktivitäten und Ressourcenkonfigurationen von Konten in Ihrer Organisation ein. Sie können diese Baseline nicht ändern, sie wird von AWS Control Tower bereitgestellt.

- Name (Name: `IdentityCenterBaseline`

  Beschreibung: Richtet gemeinsam genutzte Ressourcen für das IAM Identity Center ein, das die Einrichtung des `AWSControlTowerBaseline` Identity Center-Zugriffs für Konten vorbereitet.

  Überlegung: Diese Basislinie 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.

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 die Option Erneut registrieren oder 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.

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-Versionen

AWS Control Tower-Baselines ermöglichen es Ihnen, einen Governance-Standard auf Organisationseinheitsebene und nicht auf Ebene der Landing Zone festzulegen, wenn Ihr Unternehmen dies benötigt. Die Baseline namens `AWSControlTowerBaseline` ist verfügbar, um Ihre OUs bei AWS Control Tower zu registrieren.

> **Note**
>
> Eine Baseline ist eine Gruppe von Kontrollen und Ressourcen, die zusammenarbeiten, um eine stabile Governance-Umgebung innerhalb Ihrer Landing Zone einzurichten.

Wenn Sie eine Baseline für eine Organisationseinheit aktivieren, indem Sie die `EnableBaseline` API in AWS Control Tower aufrufen, müssen Sie eine Baseline-Version angeben, die mit Ihrer aktuellen Landing-Zone-Version von AWS Control Tower kompatibel ist. Nachdem Sie eine Baseline angegeben haben, folgen alle Mitgliedskonten in einer Organisationseinheit der Baseline, die für die Organisationseinheit angegeben ist. Mit anderen Worten, neue Konten werden mit der aktualisierten Baseline bereitgestellt und bestehende Mitgliedskonten werden gemäß der neuen Baseline verwaltet.

Wenn Sie keine Basislinie für Ihre vorhandenen OUs und Konten auswählen, bestimmt die Version der Landing Zone standardmäßig den gesamten Governance-Status. Jeder registrierten Organisationseinheit in Ihrer Landing Zone wird jedoch eine Basisversion zugewiesen, bei der es sich um die neueste Basisversion handelt, die mit Ihrer aktuellen Landing-Zone-Version kompatibel ist. Daher ist jeder Organisationseinheit und jedem registrierten Mitgliedskonto eine Baseline zugeordnet, auch wenn Sie niemals speziell eine Baseline zuweisen.

Für die Baseline auf Organisationseinheitsebene zeigt `AWSControlTowerBaseline`die folgende Tabelle die Kompatibilität von Baselines mit den Landing-Zone-Versionen von AWS Control Tower.

Basisversion	Versionen der Landing Zone	Enthaltene Vorlagen	Eingeschlossene Kontrollen	Änderung gegenüber der vorherigen Baseline	
1,0	2.0 bis 2.7	BP_BASELINE_CLOUDTRAIL,	Alle obligatorischen Kontrollen	None	

Basisversion	Versionen der Landing Zone	Enthaltene Vorlagen	Eingeschlossene Kontrollen	Änderung gegenüber der vorherigen Baseline	
		BP_BASELINE_CLOUDWATCH, BP_BASELINE_CONFIG, BP_BASELINE_ROLES, BP_BASELINE_SERVICE_ROLES, IAM-Ressourcen			
2.0	2.8 bis 2.9	BP_BASELINE_CLOUDTRAIL, BP_BASELINE_CLOUDWATCH, BP_BASELINE_CONFIG, BP_BASELINE_ROLES, BP_BASELINE_SERVICE_ROLES, Config SLR, IAM-Ressourcen	Alle obligatorischen Kontrollen	AWS Config Serviceverknüpfte Rolle (SLR) und neue Konfigurationsvorlage zur Verwendung der SLR hinzugefügt	

Basisversion	Versionen der Landing Zone	Enthaltene Vorlagen	Eingeschlossene Kontrollen	Änderung gegenüber der vorherigen Baseline	
3.0	3.0 bis 3.1	BP_BASELINE_CLOUDWATCH, BP_BASELINE_CONFIG, BP_BASELINE_ROLES, BP_BASELINE_SERVICE_ROLES, Config SLR, IAM-Ressourcen	Alle obligatorischen Kontrollen	Neuer AWS Config Blueprint. Ändern Sie , um globale Ressourcen nur in der Heimatregion aufzuzeichnen. CloudTrail Blueprint entfernt	
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	Alle obligatorischen Kontrollen	Neue SLR-Vorlage	

Weitere Informationen zu bestimmten Ressourcen, die in Konten erstellt wurden, wenn Sie Ihre Landing Zone einrichten, finden Sie unter Ressourcen, die in den freigegebenen Konten erstellt wurden.

Wenn Sie Ihre Landing Zone auf eine Version aktualisieren, die eine neuere `AWSControlTowerBaseline` Basisversion unterstützt, und die neue Landing Zone-Version mit Ihrer vorhandenen Basisversion kompatibel ist, ändert sich Ihr OU-Status in Update available .

- Sie können die Account Factory und andere Funktionen weiterhin verwenden, ohne die OU-Baseline sofort zu aktualisieren, außer im Falle einer Aktualisierung der Landing Zone von 2.x auf 3.x.
- Neue Konten, die in dieser Organisationseinheit registriert sind, erhalten Ressourcen basierend auf der vorhandenen Basisversion, bis die Basisversion aktualisiert wird (mit der Funktion Governance erweitern in der Konsole oder mithilfe der `UpdateEnabledBaseline` API).
- Nachdem Sie die Basisversion aktualisiert haben, erhalten alle Konten innerhalb dieser Organisationseinheit Ressourcen, die auf der neuen Basisversion basieren.

> **Note**
>
> Wenn Sie Ihre Landing Zone von AWS Control Tower von einer beliebigen Version 2.X auf eine beliebige Version 3.X aktualisieren, müssen Sie auch die Baseline-Version auf Ihren OUs aktualisieren, da sich von AWS CloudTrail Trails auf Kontoebene auf Organisationsebene ändert. In der Konsole zeigt Ihre Organisationseinheit den Status Update erforderlich an.

Überlegungen zu Baselines

- Wenn Ihre Organisationseinheit eine Basisaktualisierung erfordert, können Sie keine neuen Konten bereitstellen oder bestehende Konten für diese Organisationseinheit registrieren.
- Wenn Sie nach einer Aktualisierung der Landing Zone auch eine OU-Baseline aktualisieren möchten, müssen Sie die OU erneut registrieren oder Ihre OU-Baseline-Version programmgesteuert aktualisieren.
- Wir empfehlen Ihnen, für die von Ihnen verwendete Landing-Zone-Version auf die höchste kompatible Baseline 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 erhalten nicht jeden Vorteil der Landing Zone Version 3.3, 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 OUs nicht automatisch aktualisiert, wenn die übergeordnete Organisationseinheit aktualisiert wird. Wir empfehlen Ihnen, die übergeordnete Organisationseinheit zu aktualisieren, bevor Sie die verschachtelten OUs aktualisieren.
- Wenn Sie die -`UpdateEnabledBaseline`API aufrufen oder eine OU über die Konsole erneut registrieren, behält die OU alle Kontrollen bei, die vor der Baseline-Aktualisierung aktiviert wurden.
- Wenn mehrere Basisversionen mit Ihrer Landing Zone-Version kompatibel sind, müssen Sie die neueste Basisversion verwenden, wenn Sie eine Baseline für eine nicht verwaltete Organisationseinheit aktivieren, .

Beispiele: Registrieren Sie eine AWS Control Tower Tower-Organisationseinheit nur mit APIs

Bei dieser exemplarischen Vorgehensweise handelt es sich um ein Begleitdokument. Erläuterungen, Vorbehalte und weitere Informationen finden Sie unter. Arten von Basislinien

Voraussetzungen

Sie müssen über eine bestehende Organisationseinheit verfügen, die nicht bei AWS Control Tower registriert ist und die Sie registrieren möchten. Oder Sie müssen über eine registrierte Organisationseinheit verfügen, die Sie zu Aktualisierungszwecken erneut registrieren möchten.

Registrieren Sie eine Organisationseinheit

1. Prüfen Sie, ob `IdentityCenterBaseline` das für die landing zone aktiviert ist. Falls ja, rufen Sie die Identity Center Enabled Baseline-ID 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` Baseline 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`* Kennzeichen wie folgt weg:

```

aws controltower enable-baseline --baseline-identifier <AWSControlTowerBaseline ARN>
 --baseline-version <BASELINE VERSION> --target-identifier <OU ARN>
```

Registrieren Sie eine Organisationseinheit erneut

Nachdem Sie die Landingzone-Einstellungen aktualisiert oder Ihre Landingzone-Version aktualisiert haben, müssen Sie die Organisationseinheiten erneut registrieren, um ihnen die neuesten Änderungen zu geben. Gehen Sie wie folgt vor, um eine Organisationseinheit programmgesteuert erneut zu registrieren, indem Sie die zugehörige Ressource zurücksetzen. `EnabledBaseline`

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>
```

Beispiele für die API-Basisnutzung

Dieser Abschnitt enthält Beispiele für Eingabe- und Ausgabeparameter für die AWS Control Tower-Baseline-APIs .

`DisableBaseline`

Weitere Informationen zu dieser API-Operation finden Sie unter DisableBaseline.

`DisableBaseline` Eingabe:

```
{
    "enabledBaselineIdentifier": "arn:aws:controltower:us-
west-2:123456789012:enabledbaseline/AB12CD34EF56GH789"
}
```

`DisableBaseline` Ausgabe:

```
{
    "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 Informationen zu dieser API-Operation 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:

```
{
    "operationIdentifier": "58f12232-26be-4735-a3e9-dd30d90f021f",
    "arn": "arn:aws:controltower:us-west-2:123456789012:enabledbaseline/
XAHCR4CJTSI4W07MZ"
}
```

`EnableBaseline` CLI-Beispiel:

Dieses Beispiel zeigt, wie eine Baseline für eine AWS Organizations Organisation aktiviert wird, für die die Landing Zone für den Zugriff auf das AWS IAM Identity Center aktiviert ist, der von AWS Control Tower verwaltet wird. Um Ihre Identity-Center-`EnabledBaseline`ID abzurufen, können Sie die `ListEnabledBaselines`-API aufrufen und 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 werden die `EnabledBaseline` Details angezeigt, die ihre Kennung anzeigen.

```
{
    "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
```

Aktivieren Sie für eine Organisation, deren Landing Zone von der AWS Control Tower-Verwaltung von IAM Identity Center abgemeldet wurde, 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 dieser API-Operation finden Sie unter GetBaseline.

`GetBaseline` Eingabe:

```
{
    "baselineIdentifier": "arn:aws:controltower:us-west-2::baseline/17BSJV3IGJ2QSGA2"
}
```

`GetBaseline` Ausgabe:

```
{
    "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 Informationen zu dieser API-Operation finden Sie unter GetBaselineOperation.

`GetBaselineOperation` Eingabe:

```
{
    "operationIdentifier": "58f12232-26be-4735-a3e9-dd30d90f021f"
}
```

`GetBaselineOperation` Ausgabe:

```
{
    "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 Informationen zu dieser API-Operation finden Sie unter GetEnabledBaseline.

`GetEnabledBaseline` Eingabe:

```
{
    "enabledBaselineIdentifier": "arn:aws:controltower:us-
west-2:123456789012:enabledbaseline/XAHCR4CJTSI4W07MZ"
}
```

`GetEnabledBaseline` Ausgabe:

```
{
    "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 Informationen zu dieser API-Operation finden Sie unter ListBaselines.

`ListBaselines` Eingabe (mit optionalen Eingaben):

```
{
    "nextToken": "AbCd1234",
    "maxResults": "4"
}
```

`ListBaselines` Ausgabe:

```
{
    "baselines": [
        {
            "arn": "arn:aws:controltower:us-west-1::baseline/4T4HA1KMO10S6311",
            "name": "AuditBaseline",
            "description": "Sets up resources to monitor security and compliance of
 accounts in your organization."
        },
        {
            "arn": "arn:aws:controltower:us-west-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-west-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-west-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."
        }
    ]
}
```

`ListBaselines` CLI-Beispiel:

```
aws controltower list-baselines \
    --region us-west-2
```

`ListEnabledBaselines`

Weitere Informationen zu dieser API-Operation finden Sie unter ListEnabledBaselines.

`ListEnabledBaselines` Eingabe (keine Filter):

```
{
    "nextToken": "bde7-XX0c6fXXXXXX",
    "maxResults": 5
}
```

`ListEnabledBaselines` Eingabe (`baselineIdentifiers`nur 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 (`targetIdentifiers`nur 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` und `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` Ausgabe:

```
{
    "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`Filter):

```
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 dieser API-Operation finden Sie unter ResetEnabledBaseline.

`ResetEnabledbaseline` Eingabe:

```
{
    "enabledBaselineIdentifier": "arn:aws:controltower:us-
west-2:123456789012:enabledbaseline/XAJ9NKW88AA4W9CLL"
}
```

`ResetEnabledBaseline` Ausgabe:

```
{
    "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 Informationen zu dieser API-Operation 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` Ausgabe:

```
{
```

```
    "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
```

Ähnliche Informationen

In diesem Thema werden allgemeine Anwendungsfälle und bewährte Methoden für die Funktionen und zusätzliche Verbesserungen von AWS Control Tower aufgeführt. Dieses Thema enthält auch Links zu relevanten Blogbeiträgen, technischer Dokumentation und verwandten Ressourcen, die Ihnen bei der Arbeit mit AWS Control Tower helfen können.

Tutorials und Übungen

- AWS Control Tower Lab — Diese Labs bieten einen allgemeinen Überblick über allgemeine Aufgaben im Zusammenhang mit AWS Control Tower.
- Wählen Sie im AWS Control Tower Tower-Dashboard die Option Get personalisierte Beratung aus, wenn Sie einen Anwendungsfall im Sinn haben, sich aber nicht sicher sind, wo Sie anfangen sollen.
- Schauen Sie sich eine kuratierte Liste von YouTube Videos an, die mehr über die Verwendung der Funktionen von AWS Control Tower erklären.

Netzwerk

Richten Sie wiederholbare und verwaltbare Muster für Netzwerke in ein. AWS Erfahren Sie mehr über Design, Automatisierung und Geräte, die häufig von Kunden verwendet werden.

- AWS Quick Start VPC Architecture — Diese Schnellstartanleitung bietet eine Netzwerkgrundlage, die auf AWS bewährten Methoden 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 in AWS Control Tower mithilfe von AWS Service Catalog — In diesem Blogbeitrag wird beschrieben, wie Account Factory eingerichtet werden kann, sodass Sie Konten mit benutzerdefinierten VPCs bereitstellen können.
- Implementierung von Serverless Transit Network Orchestrator (STNO) in AWS Control Tower — Dieser Blogbeitrag zeigt, wie der kontenübergreifende Zugriff auf Netzwerkkonnektivität automatisiert werden kann. Dieser Blog richtet sich an AWS Control Tower Tower-Administratoren oder an Personen, die für die Netzwerkverwaltung in ihrer AWS Umgebung verantwortlich sind.

Sicherheit, Identität und Protokollierung

Erweitern Sie Ihr Sicherheitsniveau, integrieren Sie externe oder bestehende Identitätsanbieter und zentralisieren Sie Protokollierungssysteme.

Sicherheit

- Automatisieren von AWS Security Hub Warnmeldungen mit AWS Control Tower Tower-Lifecycle-Ereignissen — In diesem Blogbeitrag wird beschrieben, wie Sie die Aktivierung und Konfiguration von Security Hub in einer AWS Control Tower Tower-Umgebung mit mehreren Konten für bestehende und neue Konten automatisieren können.
- 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 es verwenden, um Konfigurationsinformationen an einem sicheren Ort für die Verwendung durch AWS Systems Manager und AWS auszutauschen CloudFormation. Sie können beispielsweise eine Liste von Regionen speichern, in denen Sie Conformance Packs 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 zentralisierte Protokollierungslösung beschrieben, mit der Unternehmen Protokolle über mehrere Konten und Regionen AWS hinweg sammeln, analysieren und anzeigen können. AWS

Bereitstellung von Ressourcen und Verwaltung von Workloads

Ressourcen und Workloads bereitstellen und verwalten.

- Erste Schritte mit der Bibliotheksintegration — In diesem Blogbeitrag werden die Portfolios „Erste Schritte“ beschrieben, die Sie verwenden können.
- Kontinuierliche Bereitstellung von Cloud Custodian auf AWS Control Tower

Arbeit mit bestehenden Organisationen und Konten

Arbeiten Sie mit bestehenden AWS Organisationen und Konten zusammen.

- Ein Konto registrieren — In diesem Thema im Benutzerhandbuch wird beschrieben, wie Sie ein vorhandenes AWS Konto bei AWS Control Tower registrieren.
- Erstellen Sie ein Konto bei AWS Control Tower — In diesem Blogbeitrag wird beschrieben, wie Sie AWS Control Tower in Ihren bestehenden AWS Organisationen einsetzen können.
- Erweitern Sie die AWS Control Tower-Governance mithilfe von AWS Config-Konformitätspaketen — In diesem Blogbeitrag wird beschrieben, wie Sie AWS Config Conformance Packs bereitstellen, um bestehende Konten und Organisationen in die Governance von AWS Control Tower zu integrieren.
- So erkennen und mindern 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 Kontrollbestimmungen 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.
- Automatisierung von Amazon VPC Flow Logs — In diesem Blogbeitrag wird beschrieben, wie Sie Amazon VPC Flow Logs in einer Umgebung mit mehreren Konten automatisieren und zentralisieren können.

- Automatisieren Sie das VPC-Tagging mit AWS Control Tower-Lifecycle-Ereignissen — In diesem Blogbeitrag wird beschrieben, wie Sie das Ressourcen-Tagging für VPCs mithilfe von Lebenszyklusereignissen in AWS Control Tower automatisieren können.
- Automatisierte Kontoverwaltung — In diesem Blogbeitrag wird beschrieben, wie Sie Kontoverwaltungsaufgaben nach der Einrichtung Ihrer AWS Control Tower Tower-Umgebung automatisieren können.

Workloads migrieren

Verwenden Sie andere AWS Services mit AWS Control Tower, um die Workload-Migration zu unterstützen.

- CloudEndure Migration — In diesem Blogbeitrag wird beschrieben, wie Sie Services CloudEndure und andere AWS Services mit AWS Control Tower kombinieren können, um die Workload-Migration zu unterstützen.

Zugehörige AWS-Services

AWS Control Tower fungiert als Orchestrierungsschicht 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 Services kann nicht direkt über die AWS Control Tower Tower-Konsole zugegriffen werden.

- Eine vollständige Liste der Services, die AWS Control Tower über AWS Organizations zur Verfügung stellt, finden Sie unter AWS-Services, die Sie mit AWS Organizations verwenden können.
- Um 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 Organizations mit anderen AWS-Services.

> **Note**
>
> Denken Sie daran, dass AWS IAM Identity Center und AWS Config, für Sie in AWS Control Tower eingerichtet und vollständig integriert AWS CloudTrail sind. Sie müssen Ihre Einstellungen für vertrauenswürdigen Zugriff oder delegierte Administration für diese Services nicht ändern.

- Einige AWS Services, die über verfügbar sind, AWS Organizations können delegierte Administration nutzen, 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 „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, mit denen Sie Software von Drittanbietern integrieren können. Diese Lösungen helfen bei der Lösung wichtiger Infrastruktur- und Betriebsanwendungsfälle, darunter Identitätsmanagement, Sicherheit für eine Umgebung mit mehreren Konten, zentralisierte Netzwerke, Operational Intelligence und Security Information and Event Management (SIEM).

Versionshinweise zu AWS Control Tower

Die folgenden Abschnitte enthalten Details zu AWS Control Tower Tower-Versionen, für die ein Update für eine AWS Control Tower Tower-Landezone erforderlich ist, sowie zu Versionen, die automatisch in den Service integriert werden.

Funktionen und Versionen werden in umgekehrter chronologischer Reihenfolge (die neuesten zuerst) aufgeführt, basierend auf dem Datum, an dem sie der Öffentlichkeit offiziell angekündigt wurden. Da es zwischen dem Zeitpunkt der Dokumentation des Features oder der Veröffentlichung und der offiziellen Ankündigung zu Verzögerungen kommen kann, kann das hier für ein Feature oder eine Veröffentlichung aufgeführte Datum geringfügig von dem Datum in abweichen. Dokumentverlauf

Funktionen, die 2024 veröffentlicht wurden

Funktionen, die 2023 veröffentlicht wurden

Funktionen, die 2022 veröffentlicht wurden

Funktionen, die 2021 veröffentlicht wurden

Im Jahr 2020 veröffentlichte Funktionen

Im Jahr 2019 veröffentlichte Funktionen

Januar 2024 - Heute

Seit Januar 2024 hat AWS Control Tower die folgenden Updates veröffentlicht:

- AWS Control Tower unterstützt bis zu 100 gleichzeitige Kontrollvorgänge
- AWS Control Tower in AWS Kanada West (Calgary) verfügbar
- AWS Control Tower unterstützt Self-Service-Kontingentanpassungen
- AWS Control Tower veröffentlicht den Controls Reference Guide
- AWS Control Tower aktualisiert und benennt zwei proaktive Kontrollen um
- Veraltete Steuerelemente sind nicht mehr verfügbar
- AWS Control Tower unterstützt das Taggen von `EnabledControl` Ressourcen in AWS CloudFormation
- AWS Control Tower unterstützt APIs für die Registrierung und Konfiguration von Organisationseinheiten mit Baselines

AWS Control Tower unterstützt bis zu 100 gleichzeitige Kontrollvorgänge

20. Mai 2024

(Für die AWS Control Tower Tower-Landezone ist kein Update erforderlich.)

AWS Control Tower unterstützt jetzt mehrere Kontrollvorgänge mit höherer Parallelität. Sie können bis zu 100 AWS Control Tower Tower-Kontrollvorgänge für mehrere Organisationseinheiten (OUs) gleichzeitig über die Konsole oder mit 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 durch sich wiederholende Kontrollvorgänge zu tragen.

Um den Status Ihrer laufenden und in der Warteschlange befindlichen Kontrollvorgänge zu überwachen, können Sie in der AWS Control Tower Tower-Konsole zur neuen Seite mit den letzten Vorgängen navigieren oder die neue `ListControlOperations`API aufrufen.

Die AWS Control Tower Tower-Bibliothek enthält mehr als 500 Kontrollen, die unterschiedlichen Kontrollzielen, Frameworks und Services zugeordnet sind. Für ein bestimmtes Kontrollziel, wie z. B. Daten im Ruhezustand verschlüsseln, können Sie mehrere Kontrollen 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 die betriebliche Komplexität.

AWS Control Tower in AWS Kanada West (Calgary) verfügbar

3. Mai 2024

(Für die AWS Control Tower Tower-Landezone ist kein Update erforderlich.)

Ab heute können Sie AWS Control Tower in der Region Kanada West (Calgary) aktivieren. Wenn Sie AWS Control Tower bereits eingesetzt haben und die Governance-Funktionen auf diese Region ausweiten möchten, können Sie dies mit den AWS Control Tower landing zone Zone-APIs tun. Oder rufen Sie von der Konsole aus die Seite Einstellungen in Ihrem AWS Control Tower Tower-Dashboard auf, 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 beinhalten, von denen in anderen Regionen.

Konten bereitstellen

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 Registrierung eines bestehenden Kontos und Schritte zur Registrierung eines Kontos.

Die Service Catalog-APIs sind in der Region Kanada West (Calgary) nicht verfügbar. Das in Automate Account Provisioning in AWS Control Tower by Service Catalog APIs gezeigte 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 andere zugrunde liegende Abhängigkeiten für AWS Control Tower fehlen. Wenn Sie die Verwaltung auf die Region Kanada West (Calgary) ausweiten, 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 Service-Managed Standard: AWS Control Tower sind in der Region Kanada West (Calgary) nicht verfügbar. Die präventive Kontrolle `CT.CLOUDFORMATION.PR.1` ist in Canada West (Calgary) nicht verfügbar, da sie nur für die Aktivierung der hakenbasierten, proaktiven Kontrollen erforderlich ist. Bestimmte detektive Kontrollen, die auf basieren, AWS Config sind nicht verfügbar. Details hierzu finden Sie unter Einschränkungen der Kontrolle.

Identitätsanbieter

IAM Identity Center ist in Canada West (Calgary) nicht verfügbar. Es empfiehlt sich, Ihre landing zone 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 von 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 AWS Control Tower Tower-Landezone ist kein Update erforderlich.)

AWS Control Tower unterstützt jetzt Self-Service-Kontingentanpassungen über die Service Quotas Quotas-Konsole. Weitere Informationen finden Sie unter Anfordern einer Kontingenterhöhung.

AWS Control Tower veröffentlicht den Controls Reference Guide

21. April 2024

(Für die AWS Control Tower Tower-Landezone ist kein Update erforderlich.)

AWS Control Tower hat den Controls Reference Guide veröffentlicht, ein neues Dokument, in dem Sie detaillierte Informationen zu den Kontrollen finden, die für die AWS Control Tower Tower-Umgebung spezifisch sind. Zuvor war dieses Material im AWS Control Tower Tower-Benutzerhandbuch enthalten. Das Referenzhandbuch für Steuerungen behandelt Steuerungen in einem erweiterten Format. Weitere Informationen finden Sie im Referenzhandbuch zu AWS Control Tower Controls.

AWS Control Tower aktualisiert und benennt zwei proaktive Kontrollen um

26. März 2024

(Für die AWS Control Tower Tower-Landezone ist kein Update erforderlich.)

AWS Control Tower hat zwei proaktive Kontrollen umbenannt, um sie an die Aktualisierungen von Amazon OpenSearch Service anzupassen.

- [CT.OPENSEARCH.PR.8] Für die Verwendung von TLSv1.2 ist eine Elasticsearch Service-Domain erforderlich
- [CT.OPENSEARCH.PR.16] Für die Verwendung von TLSv1.2 ist eine Amazon OpenSearch Service-Domain erforderlich

Wir haben die Kontrollnamen und die Artefakte für diese beiden Kontrollen aktualisiert, um sie an die aktuelle Version von Amazon OpenSearch Service anzupassen, die jetzt Transport Layer Security

(TLS) Version 1.3 als Teil seiner Transportsicherheitsoptionen für die Domain-Endpunktsicherheit unterstützt.

Um die Unterstützung für TLSv1.3 für diese Steuerelemente hinzuzufügen, haben wir das Artefakt und den Namen der Kontrollen aktualisiert, sodass sie der Absicht der Steuerung entsprechen. Sie bewerten jetzt die TLS-Mindestversion der Dienstdomäne. Um dieses Update in Ihrer Umgebung durchzuführen, müssen Sie die Steuerelemente deaktivieren und aktivieren, um das neueste Artefakt bereitzustellen.

Keine anderen proaktiven Kontrollen 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 AWS Control Tower Tower-Landezone ist kein Update erforderlich.)

AWS Control Tower hat einige Kontrollen als veraltet eingestuft. Diese Steuerungen 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 AWS CloudFormation

22. Februar 2024

(Für die AWS Control Tower Tower-Landezone ist kein Update erforderlich.)

Diese AWS Control Tower Tower-Version aktualisiert das Verhalten der `EnabledControl` Ressource, um es besser an konfigurierbare Kontrollen anzupassen und die Fähigkeit zu verbessern, Ihre AWS Control Tower Tower-Umgebung mit Automatisierung zu verwalten. Mit dieser Version können Sie mithilfe von AWS CloudFormation Vorlagen Tags zu konfigurierbaren `EnabledControl` Ressourcen hinzufügen. Bisher konnten Sie Tags nur über die AWS Control Tower Tower-Konsole und APIs hinzufügen.

Der AWS Control Tower `GetEnabledControl` und die `ListTagsforResource` API-Operationen werden mit dieser Version aktualisiert, da sie von der `EnabledControl` Ressourcenfunktionalität abhängen. `EnableControl`

Weitere Informationen finden Sie unter `EnabledControl`Tagging-Ressourcen in AWS Control Tower und `EnabledControl`im AWS CloudFormation Benutzerhandbuch.

AWS Control Tower unterstützt APIs für die Registrierung und Konfiguration von Organisationseinheiten mit Baselines

14. Februar 2024

(Für die AWS Control Tower Tower-Landezone ist kein Update erforderlich.)

Diese APIs unterstützen die programmatische Registrierung von Organisationseinheiten beim `EnableBaseline` Anruf. Wenn Sie eine Baseline für eine OU aktivieren, werden Mitgliedskonten innerhalb der OU bei AWS Control Tower Governance registriert. Es können bestimmte Vorbehalte gelten. Beispielsweise ermöglicht die OU-Registrierung über die AWS Control Tower Tower-Konsole sowohl optionale als auch obligatorische Kontrollen. Beim Aufrufen von APIs müssen Sie möglicherweise einen zusätzlichen Schritt ausführen, damit optionale Steuerungen aktiviert werden.

Eine AWS Control Tower Tower-Baseline beinhaltet bewährte Methoden für die AWS Control Tower Tower-Governance einer Organisationseinheit und Mitgliedskonten. Wenn Sie beispielsweise eine Baseline für eine Organisationseinheit aktivieren, erhalten Mitgliedskonten innerhalb der Organisationseinheit eine definierte Gruppe von Ressourcen AWS CloudTrail AWS Config, einschließlich IAM Identity Center und den erforderlichen AWS IAM-Rollen.

Bestimmte Baselines sind mit bestimmten Versionen der AWS Control Tower landing zone kompatibel. AWS Control Tower kann die neueste kompatible Baseline auf Ihre landing zone anwenden, wenn Sie Ihre Landezone-Einstellungen ändern. Weitere Informationen finden Sie unter Kompatibilität von OU-Baselines und Landing-Zone-Versionen.

Diese Version enthält vier wichtige Arten von Basislinien

- `AWSControlTowerBaseline`
- `AuditBaseline`
- `LogArchiveBaseline`
- `IdentityCenterBaseline`

Mit den neuen APIs und definierten Baselines können Sie OUs registrieren und Ihren OU-Bereitstellungs-Workflow automatisieren. Die APIs können auch Organisationseinheiten verwalten, die bereits unter der Kontrolle von AWS Control Tower stehen, sodass Sie OUs nach landing zone Zone-Updates erneut registrieren können. Die APIs bieten Unterstützung für eine AWS CloudFormation `EnabledBaseline` Ressource, mit der Sie Ihre Organisationseinheiten mit Infrastructure as Code (IaC) verwalten können.

Basis-APIs

- EnableBaseline, UpdateEnabledBaseline, DisableBaseline: Ergreifen Sie Maßnahmen auf der Grundlage einer Basisversion für eine Organisationseinheit.
- GetEnabledBaseline, ListEnabledBaselines: Entdecken Sie Konfigurationen für Ihre aktivierten Baselines.
- GetBaselineOperation: Zeigt den Status eines bestimmten Basisvorgangs an.
- ResetEnabledBaseline: Korrigiert Ressourcenverschiebungen auf einer Organisationseinheit mit aktivierter Baseline (einschließlich verschachtelter Organisationseinheiten und obligatorischer Kontrollabweichungen). Behebt auch Drift bei der Deny-Control-Einstellung in der Region landing-zone-level
- GetBaseline, ListBaselines: Entdecken Sie den Inhalt der AWS Control Tower Tower-Baselines.

Weitere Informationen zu diesen APIs finden Sie unter Baselines im AWS Control Tower Tower-Benutzerhandbuch und in der API-Referenz. Die neuen APIs sind dort verfügbar AWS-Regionen , wo AWS Control Tower verfügbar ist, mit Ausnahme der Regionen GovCloud (USA). Eine Liste, AWS-Regionen wo AWS Control Tower verfügbar ist, finden Sie in der AWS-Region Tabelle.

Januar 2023 — Heute

Seit Januar 2023 hat AWS Control Tower die folgenden Updates veröffentlicht:

- Übergang zum neuen AWS Service Catalog externen Produkttyp (Phase 3)
- AWS-Control-Tower-Landezone, Version 3.3
- Umstellung auf einen neuen AWS Service Catalog externen Produkttyp (Phase 2)
- AWS Control Tower kündigt Kontrollen zur Unterstützung der digitalen Souveränität an
- AWS Control Tower unterstützt Landingzone-APIs
- AWS Control Tower unterstützt Tagging für aktivierte Kontrollen
- AWS Control Tower in der Region Asien-Pazifik (Melbourne) verfügbar
- Umstellung auf den neuen AWS Service Catalog externen Produkttyp (Phase 1)
- Neue Kontroll-API verfügbar
- AWS Control Tower fügt zusätzliche Kontrollen hinzu
- Es wurde ein neuer Drift-Typ gemeldet: Vertrauenswürdiger Zugriff deaktiviert
- Vier weitere AWS-Regionen
- AWS Control Tower in der Region Tel Aviv verfügbar
- AWS Control Tower führt 28 neue proaktive Kontrollen ein
- AWS Control Tower lehnt zwei Kontrollen ab
- AWS-Control-Tower-Landezone, Version 3.2
- AWS Control Tower verwaltet Konten auf der Grundlage von IDs
- Zusätzliche Security Hub Hub-Detektivkontrollen sind in der AWS Control Tower Tower-Steuerungsbibliothek verfügbar
- AWS Control Tower veröffentlicht Tabellen mit Kontrollmetadaten
- Terraform-Unterstützung für Account Factory Customization
- AWS IAM Identity Center-Selbstmanagement für die landing zone verfügbar
- AWS Control Tower befasst sich mit gemischter Governance für Organisationseinheiten
- Zusätzliche proaktive Kontrollen verfügbar
- Aktualisierte proaktive Amazon EC2 EC2-Kontrollen
- AWS-Regionen Sieben weitere verfügbar
- Rückverfolgung von Anfragen zur Kontoanpassung von Account Factory for Terraform (AFT)
- AWS-Control-Tower-Landezone, Version 3.1
- Proaktive Kontrollen sind allgemein verfügbar

Übergang zum neuen AWS Service Catalog externen Produkttyp (Phase 3)

14. Dezember 2023

(Für die AWS Control Tower Tower-Landezone 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 Umstellung auf den AWS Service Catalog Produkttyp Extern.

Wenn Sie Ihre Konto-Blueprints nicht aktualisieren, um den Produkttyp Extern zu verwenden, können Sie nur Konten aktualisieren oder kündigen, die Sie mit Terraform Open Source-Blueprints bereitgestellt haben.

AWS-Control-Tower-Landezone, Version 3.3

14. Dezember 2023

(Für die AWS Control Tower landing zone ist ein Update auf Version 3.3 erforderlich. Weitere Informationen finden Sie unterAktualisieren Ihrer Landing Zone).

Aktualisierungen der S3-Bucket-Richtlinie im AWS Control Tower Audit-Konto

Wir haben die Amazon S3 S3-Audit-Bucket-Richtlinie, die AWS Control Tower in Konten bereitstellt, geändert, sodass eine `aws:SourceOrgID` Bedingung für alle Schreibberechtigungen erfüllt sein muss. Mit 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. Dadurch wird 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 im Auditkonto

Weitere Informationen zum neuen Bedingungsschlüssel finden Sie in der IAM-Dokumentation und im IAM-Blogbeitrag mit dem Titel „Verwenden Sie skalierbare Kontrollen 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. Die aktualisierte Richtlinie finden Sie unter Die AWS Config SNS-Themenrichtlinie.

Aktualisierungen der Steuerung „Region Deny“ für die landing zone

- Entferntdiscovery-marketplace:. Diese Maßnahme fällt unter die `aws-marketplace:*` Ausnahmeregelung.
- `quicksight:DescribeAccountSubscription` hinzugefügt

AWS CloudFormation Vorlage wurde aktualisiert

Wir haben die AWS CloudFormation Vorlage für den genannten Stack `BASELINE-CLOUDTRAIL-MASTER` so aktualisiert, dass sie keine Drift zeigt, wenn keine AWS KMS Verschlüsselung verwendet wird.

Umstellung auf einen neuen AWS Service Catalog externen Produkttyp (Phase 2)

7. Dezember 2023

(Für die AWS Control Tower 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 bestehenden Workloads und AWS Ressourcen in Ihren Konten zu vermeiden, folgen Sie bis zum 14. Dezember 2023 den Schritten zur Umstellung auf den Produkttyp AWS Service Catalog External auf AWS Control Tower.

AWS Control Tower kündigt Kontrollen zur Unterstützung der digitalen Souveränität an

27. November 2023

(Für die AWS Control Tower Tower-Landezone ist kein Update erforderlich.)

AWS Control Tower kündigt 65 neue AWS verwaltete Kontrollen an, mit denen Sie Ihre Anforderungen an digitale Souveränität erfüllen können. Mit dieser Version können Sie diese Kontrollen unter einer neuen Gruppe für digitale Souveränität in der AWS Control Tower Tower-Konsole entdecken. Sie können diese Kontrollen verwenden, um Aktionen zu verhindern und Ressourcenänderungen in Bezug auf Datenresidenz, granulare Zugriffsbeschränkung, Verschlüsselung und Ausfallsicherheit zu erkennen. Diese Kontrollen sollen es Ihnen erleichtern, Anforderungen in großem Umfang zu erfüllen. Weitere Informationen zu Kontrollen der digitalen Souveränität finden Sie unter Kontrollen, die den Schutz der digitalen Souveränität verbessern.

Sie können sich beispielsweise dafür entscheiden, Kontrollen zu aktivieren, mit denen Sie Ihre Verschlüsselungs- und Ausfallsicherheitsstrategien durchsetzen können, wie z. B. Erfordern Sie, dass ein AWS AppSync API-Cache erforderlich ist, um die Verschlüsselung bei der Übertragung zu aktivieren, oder Erfordern, dass eine AWS Network Firewall in mehreren Availability Zones bereitgestellt wird. Sie können auch die AWS Control Tower Region Deny Control so anpassen, dass regionale Einschränkungen angewendet werden, die Ihren individuellen Geschäftsanforderungen am besten entsprechen.

Diese Version bietet deutlich verbesserte Funktionen zum Ablehnen von AWS Control Tower Region. Sie können eine neue, parametrisierte Regionsverweigerungskontrolle auf OU-Ebene anwenden, um die Granularität der Steuerung zu erhöhen und gleichzeitig zusätzliche Region-Governance auf Landing-Zone-Ebene beizubehalten. Diese anpassbare Regionsverweigerungssteuerung hilft Ihnen dabei, regionale Beschränkungen anzuwenden, die Ihren individuellen Geschäftsanforderungen am besten entsprechen. Weitere Informationen zur neuen, konfigurierbaren Regionsverweigerungssteuerung finden Sie unter Auf die Organisationseinheit angewendete Regionsverweigerungssteuerung.

Als neues Tool für die neue Erweiterung „Region Deny“ enthält diese Version eine neue API`UpdateEnabledControl`, mit der Sie Ihre aktivierten Kontrollen 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: Erfordert, dass eine Amazon API Gateway Gateway-REST-Domain eine Sicherheitsrichtlinie verwendet, die eine Mindestversion des TLS-Protokolls von TLSv1.2 festlegt

- 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 ist
- 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 Scaling-Startkonfiguration konfiguriert wurde, um Daten im Ruhezustand zu verschlüsseln
- CT.AUTOSCALING.PR.10: Erfordert, dass eine Amazon EC2 Auto Scaling Scaling-Gruppe nur AWS Nitro-Instance-Typen verwendet, wenn eine Startvorlage überschrieben wird
- CT.AUTOSCALING.PR.11: Erfordert, dass nur AWS Nitro-Instance-Typen, die die Verschlüsselung des Netzwerkverkehrs zwischen Instances unterstützen, zu einer Amazon EC2 Auto Scaling Scaling-Gruppe hinzugefügt werden, wenn eine Startvorlage überschrieben wird
- CT.DAX.PR.3: Erfordert einen DynamoDB Accelerator-Cluster, um Daten während 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 EC2-Instance einen AWS Nitro-Instance-Typ verwendet, wenn sie aus dem `AWS::EC2::LaunchTemplate` Ressourcentyp erstellt
- CT.EC2.PR.16: Erfordert, dass eine Amazon EC2 EC2-Instance einen AWS Nitro-Instance-Typ verwendet, wenn sie mit dem `AWS::EC2::Instance` Ressourcentyp erstellt wurde
- CT.EC2.PR.17: Für die Verwendung eines AWS-Nitro-Instance-Typs ist ein dedizierter Amazon EC2 EC2-Host erforderlich
- CT.EC2.PR.18: Erfordert, dass eine Amazon EC2 EC2-Flotte nur die Startvorlagen mit AWS Nitro-Instance-Typen überschreibt
- CT.EC2.PR.19: Erfordert, dass eine Amazon EC2 EC2-Instance einen Nitro-Instance-Typ verwendet, der die Verschlüsselung während der Übertragung zwischen Instances unterstützt, wenn sie mit dem Ressourcentyp erstellt wurde `AWS::EC2::Instance`
- CT.EC2.PR.20: Erfordert, dass eine Amazon EC2 EC2-Flotte nur die Startvorlagen mit AWS Nitro-Instance-Typen überschreibt, die die Verschlüsselung bei der Übertragung zwischen Instances unterstützen

- CT.ELASTICACHE.PR.8: Für eine ElastiCache Amazon-Replikationsgruppe späterer Redis-Versionen muss die RBAC-Authentifizierung aktiviert sein
- CT.MQ.PR.1: Erfordert, dass ein Amazon MQ ActiveMQ-Broker den Aktiv-/Standby-Bereitstellungsmodus für hohe Verfügbarkeit verwendet
- CT.MQ.PR.2: Erfordert einen Amazon MQ Rabbit MQ-Broker, der den Multi-AZ-Clustermodus für hohe Verfügbarkeit verwendet
- CT.MSK.PR.1: Erfordert einen Amazon Managed Streaming for Apache Kafka (MSK) -Cluster, um die Verschlüsselung bei der Übertragung zwischen Cluster-Broker-Knoten zu erzwingen
- CT.MSK.PR.2: Erfordert die Konfiguration eines Amazon Managed Streaming for Apache Kafka (MSK) -Clusters mit deaktivierter Option PublicAccess
- CT.NETWORK-FIREWALL.PR.5: Erfordert, dass eine AWS Netzwerk-Firewall-Firewall in mehreren Availability Zones bereitgestellt wird
- CT.RDS.PR.26: Erfordert einen Amazon RDS-DB-Proxy, um Transport Layer Security (TLS) -Verbindungen zu benötigen
- CT.RDS.PR.27: Erfordert eine Amazon RDS-DB-Cluster-Parametergruppe, die Transport Layer Security (TLS) -Verbindungen für unterstützte Engine-Typen erfordert
- CT.RDS.PR.28: Erfordert eine Amazon RDS-DB-Parametergruppe, die Transport Layer Security (TLS) -Verbindungen für unterstützte Engine-Typen erfordert
- 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: Für einen Amazon S3 S3-Zugriffspunkt ist eine Block Public Access (BPA) -Konfiguration erforderlich, bei der alle Optionen auf true gesetzt sind

Neue präventive Kontrollen

- CT.APPSYNC.PV.1Erfordern, dass eine AWS AppSync GraphQL-API mit privater Sichtbarkeit konfiguriert ist
- CT.EC2.PV.1Erfordern, dass ein Amazon EBS-Snapshot aus einem verschlüsselten EC2-Volume erstellt wird
- CT.EC2.PV.2Erfordern, dass ein angehängtes Amazon EBS-Volume so konfiguriert ist, dass Daten im Ruhezustand verschlüsselt werden

- CT.EC2.PV.3Erfordern, dass ein Amazon EBS-Snapshot nicht öffentlich wiederherstellbar ist
- CT.EC2.PV.4Erfordern, dass direkte Amazon EBS-APIs nicht aufgerufen werden
- CT.EC2.PV.5Die Verwendung von Amazon EC2 EC2-VM-Import und -Export verbieten
- CT.EC2.PV.6Die Verwendung veralteter Amazon RequestSpotFleet EC2- und API-Aktionen verbieten 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, dass ein AWS KMS asymmetrischer Schlüssel mit RSA-Schlüsselmaterial, der 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 zur Sperrung der Umgehungsrichtlinie aktiviert ist
- CT.KMS.PV.4Erfordern, 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 ist
- CT.KMS.PV.6Erfordern Sie, dass AWS KMS ein vom Kunden verwalteter Schlüssel (CMK) mit Schlüsselmaterial konfiguriert ist, das aus einem externen Schlüsselspeicher (XKS) stammt
- CT.LAMBDA.PV.1Für die Verwendung der IAM-basierten AWS Lambda Authentifizierung ist eine Funktions-URL erforderlich AWS
- CT.LAMBDA.PV.2Erfordern Sie, dass eine AWS Lambda Funktions-URL für den Zugriff nur durch Principals in Ihrem AWS-Konto
- CT.MULTISERVICE.PV.1: Verweigern Sie den Zugriff auf AWS basierend auf der für eine Organisationseinheit angeforderten AWS-Region

Die neuen detektivischen Kontrollen, die Ihre Kontrolle über digitale Souveränität verbessern, sind Teil des AWS Security Hub Service-Managed Standard AWS Control Tower.

Neue detektivische Kontrollen

- SH.ACM.2: Von ACM verwaltete RSA-Zertifikate sollten eine Schlüssellänge von mindestens 2.048 Bit verwenden
- SH.AppSync.5: AWS AppSync GraphQL-APIs sollten nicht mit API-Schlüsseln authentifiziert werden

- SH.CloudTrail.6: Stellen Sie sicher, dass der zum Speichern von CloudTrail Protokollen verwendete S3-Bucket nicht öffentlich zugänglich ist:
- SH.DMS.9: DMS-Endpunkte sollten SSL verwenden
- SH.DocumentDB.3: Manuelle Cluster-Snapshots von Amazon DocumentDB sollten nicht öffentlich sein
- SH.DynamoDB.3: DynamoDB Accelerator (DAX) -Cluster sollten im Ruhezustand verschlüsselt werden
- SH.EC2.23: EC2 Transit Gateways sollten VPC-Anhangsanfragen nicht automatisch akzeptieren
- SH.EKS.1: EKS-Cluster-Endpunkte sollten nicht öffentlich zugänglich sein
- SH.ElastiCache.3: Für ElastiCache Replikationsgruppen sollte automatisches Failover aktiviert sein
- SH.ElastiCache.4: Für ElastiCache Replikationsgruppen hätte aktiviert werden müssen encryption-at-rest
- SH.ElastiCache.5: ElastiCache Replikationsgruppen hätten encryption-in-transit aktiviert sein müssen
- SH.ElastiCache.6: Für ElastiCache Replikationsgruppen früherer Redis-Versionen sollte Redis AUTH aktiviert sein
- SH.EventBridge.3: An EventBridge benutzerdefinierte Event-Busse sollte eine ressourcenbasierte Richtlinie angehängt sein
- SH.KMS.4: Die AWS KMS Schlüsselrotation sollte aktiviert sein
- SH.Lambda.3: Lambda-Funktionen sollten sich in einer VPC befinden
- SH.MQ.5: ActiveMQ-Broker sollten den Aktiv-/Standby-Bereitstellungsmodus verwenden
- SH.MQ.6: RabbitMQ-Broker sollten den Cluster-Bereitstellungsmodus verwenden
- SH.MSK.1: MSK-Cluster sollten bei der Übertragung zwischen Broker-Knoten verschlüsselt werden
- SH.RDS.12: Die IAM-Authentifizierung sollte für RDS-Cluster konfiguriert werden
- SH.RDS.15: RDS-DB-Cluster sollten für mehrere Availability Zones konfiguriert werden
- SH.S3.17: S3-Buckets sollten im Ruhezustand mit AWS KMS Schlüsseln verschlüsselt werden

Weitere Informationen zu den Kontrollen, die dem AWS Security Hub Service-Managed Standard AWS Control Tower hinzugefügt wurden, finden Sie in der Dokumentation unter Kontrollen, die für den AWS Security Hub Service-Managed Standard gelten: AWS Control Tower.

Eine Liste der Kontrollen AWS-Regionen , die Teil des AWS Security Hub Service-Managed Standard AWS Control Tower sind, nicht unterstützen, finden Sie unter Nicht unterstützte Regionen.

Neue konfigurierbare Steuerung für Regionsverweigerung auf OU-Ebene

CT.MULTISERVICE.PV.1: Dieses Steuerelement akzeptiert Parameter zur Angabe ausgenommener Regionen, IAM-Prinzipale und Aktionen, die auf OU-Ebene und nicht für die gesamte AWS Control Tower Tower-Landezone zulässig sind. Es handelt sich um eine präventive Kontrolle, die durch eine Service Control Policy (SCP) implementiert wird.

Weitere Informationen finden Sie unter Anwendung der auf die Organisationseinheit angewendeten Regionsverweigerungssteuerung.

Die **`UpdateEnabledControl`**-API

Diese AWS Control Tower Tower-Version bietet die folgende API-Unterstützung für Steuerungen:

- Die aktualisierte `EnableControl` API kann konfigurierbare Steuerungen konfigurieren.
- Die aktualisierte `GetEnabledControl` API zeigt die konfigurierten Parameter eines aktivierten Steuerelements an.
- Die neue `UpdateEnabledControl` API kann die Parameter eines aktivierten Steuerelements ändern.

Weitere Informationen finden Sie in der AWS Control Tower API-Referenz.

AWS Control Tower unterstützt Landingzone-APIs

26. November 2023

(Für die AWS Control Tower Tower-Landezone ist kein Update erforderlich.)

AWS Control Tower unterstützt jetzt die Konfiguration und den Start von landing zone mithilfe von APIs. Sie können Landing Zones mithilfe von APIs erstellen, aktualisieren, abrufen, auflisten, zurücksetzen und löschen.

Mit den folgenden APIs können Sie Ihre landing zone programmatisch einrichten und verwalten, indem Sie AWS CloudFormation oder die AWS CLI.

AWS Control Tower unterstützt die folgenden APIs für Landezonen:

- `CreateLandingZone`— Dieser API-Aufruf erstellt eine landing zone mithilfe einer Landingzone-Version und einer Manifestdatei.

- `GetLandingZoneOperation`— Dieser API-Aufruf gibt den Status einer angegebenen Landezonenoperation zurück.
- `GetLandingZone`— Dieser API-Aufruf gibt Details zur angegebenen landing zone zurück, einschließlich Version, Manifestdatei und Status.
- `UpdateLandingZone`— Dieser API-Aufruf aktualisiert die Landingzone-Version oder die Manifestdatei.
- `ListLandingZone`— Dieser API-Aufruf gibt eine landing zone Identifier (ARN) für eine Landingzone-Einrichtung im Verwaltungskonto zurück.
- `ResetLandingZone`— Dieser API-Aufruf setzt die landing zone auf die beim letzten Update angegebenen Parameter zurück, wodurch Drift behoben werden kann. Wenn die landing zone nicht aktualisiert wurde, setzt dieser Aufruf die landing zone auf die bei der Erstellung angegebenen Parameter zurück.
- `DeleteLandingZone`—Dieser API-Aufruf setzt die landing zone außer Betrieb.

Informationen zu den ersten Schritten mit Landingzone-APIs finden Sie unterErste Schritte mit AWS Control Tower mithilfe von APIs.

AWS Control Tower unterstützt Tagging für aktivierte Kontrollen

10. November 2023

(Für die AWS Control Tower Tower-Landezone ist kein Update erforderlich.)

AWS Control Tower unterstützt jetzt Ressourcen-Tagging für aktivierte Kontrollen über die AWS Control Tower Tower-Konsole oder über APIs. Sie können Tags für aktivierte Kontrollen hinzufügen, entfernen oder auflisten.

Mit der Veröffentlichung der folgenden APIs können Sie Tags für die Kontrollen konfigurieren, die Sie in AWS Control Tower aktivieren. Mithilfe von Tags können Sie Ressourcen verwalten, identifizieren, organisieren, suchen und filtern. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren.

AWS Control Tower unterstützt die folgenden APIs für das Kontroll-Tagging:

- `TagResource`— Dieser API-Aufruf fügt Tags zu den in AWS Control Tower aktivierten Steuerelementen hinzu.
- `UntagResource`— Dieser API-Aufruf entfernt Tags aus Steuerelementen, die in AWS Control Tower aktiviert sind.

- `ListTagsForResource`— Dieser API-Aufruf gibt Tags für Kontrollen zurück, die in AWS Control Tower aktiviert sind.

AWS Control Tower-Steuerungs-APIs sind dort verfügbar AWS-Regionen , wo AWS Control Tower verfügbar ist. Eine vollständige Liste der Länder, AWS-Regionen in denen AWS Control Tower verfügbar ist, finden Sie in der AWS Regionstabelle. Eine vollständige Liste der AWS Control Tower Tower-APIs finden Sie in der API-Referenz.

AWS Control Tower in der Region Asien-Pazifik (Melbourne) verfügbar

3. November 2023

(Für die AWS Control Tower Tower-Landezone ist kein Update erforderlich.)

AWS Control Tower ist in der Region Asien-Pazifik (Melbourne) verfügbar.

Wenn Sie AWS Control Tower bereits verwenden und die Governance-Funktionen in Ihren Konten auf diese Region ausweiten möchten, gehen Sie in Ihrem AWS Control Tower Tower-Dashboard zur Seite Einstellungen, wählen Sie die Region aus und aktualisieren Sie dann Ihre landing zone. Nach einem landing zone Zone-Update müssen Sie alle Konten aktualisieren, die von AWS Control Tower verwaltet werden, um Ihre Konten und Organisationseinheiten in der neuen Region unter Kontrolle zu bringen. Weitere Informationen finden Sie unter Über Updates.

Eine vollständige Liste der Regionen, in denen AWS Control Tower verfügbar ist, finden Sie in der AWS-Region Tabelle.

Umstellung auf den neuen AWS Service Catalog externen Produkttyp (Phase 1)

31. Oktober 2023

(Für die AWS Control Tower 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 aktualisiert.

AWS Control Tower unterstützt keine Account Factory Factory-Anpassungen, die auf dem AWS Service Catalog externen Produkttyp basieren. Um eine Unterbrechung der bestehenden Workloads

und AWS Ressourcen in Ihren Konten zu vermeiden, befolgen Sie die Schritte zur Umstellung auf AWS Control Tower bis zum 14. Dezember 2023 in dieser empfohlenen Reihenfolge:

1. Aktualisieren Sie Ihre bestehende Terraform Reference Engine, sodass AWS Service Catalog sie Unterstützung sowohl für externe als auch für Terraform Open Source-Produkttypen bietet. Anweisungen zur Aktualisierung Ihrer Terraform Reference Engine finden Sie im Repository.AWS Service Catalog GitHub
2. Gehen Sie zu allen vorhandenen Terraform Open Source-Blueprints AWS Service Catalog und duplizieren Sie sie, um den neuen externen Produkttyp zu verwenden. Beenden Sie nicht die vorhandenen Terraform Open Source-Blueprints.
3. Verwenden Sie weiterhin Ihre vorhandenen Terraform Open Source-Blueprints, um Konten in AWS Control Tower zu erstellen oder zu aktualisieren.

Neue Kontroll-API verfügbar

14. Oktober 2023

(Für die AWS Control Tower Tower-Landezone ist kein Update erforderlich.)

AWS Control Tower unterstützt jetzt eine zusätzliche API, mit der Sie Ihre AWS Control Tower Tower-Steuerungen in großem Umfang bereitstellen und verwalten können. Weitere Informationen zu den AWS Control Tower Control APIs finden Sie in der API-Referenz.

AWS Control Tower hat eine neue Kontroll-API hinzugefügt.

- `GetEnabledControl`— Der API-Aufruf liefert Details zu einer aktivierten Steuerung.

Wir haben auch diese API aktualisiert:

`ListEnabledControls`— Dieser API-Aufruf listet die von AWS Control Tower für die angegebene Organisationseinheit aktivierten Kontrollen und die darin enthaltenen Konten auf. Es gibt jetzt zusätzliche Informationen in einem `EnabledControlSummary` Objekt zurück.

Mit diesen APIs können Sie mehrere gängige Operationen programmgesteuert ausführen. Beispielsweise:

- Rufen Sie eine Liste aller von Ihnen aktivierten Steuerungen aus der AWS Control Tower Tower-Steuerungsbibliothek ab.

- Für jedes aktivierte Steuerelement können Sie Informationen über die Regionen abrufen, in denen das Steuerelement unterstützt wird, die Kennung (ARN) des Steuerelements, den Driftstatus des Steuerelements und die Statusübersicht des Steuerelements.

AWS Control Tower-Steuerungs-APIs sind dort verfügbar AWS-Regionen , wo AWS Control Tower verfügbar ist. Eine vollständige Liste der Länder, AWS-Regionen in denen AWS Control Tower verfügbar ist, finden Sie in der AWS Regionstabelle. Eine vollständige Liste der AWS Control Tower Tower-APIs finden Sie in der API-Referenz.

AWS Control Tower fügt zusätzliche Kontrollen hinzu

5. Oktober 2023

(Für die AWS Control Tower Tower-Landezone ist kein Update erforderlich.)

AWS Control Tower kündigt neue proaktive und detektive Kontrollen an.

Proaktive Kontrollen in AWS Control Tower werden mithilfe von AWS CloudFormation Hooks implementiert, die nicht konforme Ressourcen identifizieren und blockieren, bevor sie bereitgestellt AWS CloudFormation werden. Proaktive Kontrollen ergänzen die bestehenden präventiven und detektiven Kontrollfunktionen in AWS Control Tower.

Neue proaktive Kontrollen

- [CT.ATHENA.PR.1] Erfordert eine Amazon Athena Athena-Arbeitsgruppe, um Athena-Abfrageergebnisse im Ruhezustand zu verschlüsseln
- [CT.ATHENA.PR.2] Eine Amazon Athena Athena-Arbeitsgruppe auffordern, Athena-Abfrageergebnisse im Ruhezustand mit einem AWS Key Management Service (KMS-) Schlüssel zu verschlüsseln
- [CT.CLOUDTRAIL.PR.4] Erfordert einen AWS CloudTrail Lake-Event-Datenspeicher, um die Verschlüsselung im Ruhezustand mit einem Schlüssel zu aktivieren AWS KMS
- [CT.DAX.PR.2] Erfordert einen Amazon DAX-Cluster, um Knoten in mindestens drei Availability Zones bereitzustellen
- [CT.EC2.PR.14] Erfordert ein Amazon EBS-Volume, das über eine Amazon EC2 EC2-Startvorlage konfiguriert wurde, um Daten im Ruhezustand zu verschlüsseln
- [CT.EKS.PR.2] Erfordert, dass ein Amazon EKS-Cluster mit geheimer Verschlüsselung mithilfe von AWS Key Management Service (KMS) -Schlüsseln konfiguriert wird

- [CT.ELASTICLOADBALANCING.PR.14] Zonenübergreifendes Load Balancing muss über einen Network Load Balancer aktiviert sein
- [CT.ELASTICLOADBALANCING.PR.15] Erfordern, dass eine Elastic Load Balancing v2-Zielgruppe den zonenübergreifenden Load Balancing nicht explizit deaktiviert
- [CT.EMR.PR.1] Erfordert, dass eine Amazon EMR (EMR) -Sicherheitskonfiguration konfiguriert ist, um ruhende Daten in Amazon S3 zu verschlüsseln
- [CT.EMR.PR.2] Erfordert, dass eine Amazon EMR (EMR) -Sicherheitskonfiguration so konfiguriert ist, dass ruhende Daten in Amazon S3 mit einem Schlüssel verschlüsselt werden AWS KMS
- [CT.EMR.PR.3] Erfordert, dass eine Amazon EMR (EMR) -Sicherheitskonfiguration mit EBS-Volume und lokaler Festplattenverschlüsselung unter Verwendung eines Schlüssels konfiguriert ist AWS KMS
- [CT.EMR.PR.4] Erfordert, dass eine Amazon EMR (EMR) -Sicherheitskonfiguration konfiguriert ist, um Daten während der Übertragung zu verschlüsseln
- [CT.GLUE.PR.1] Erfordert, dass ein AWS Glue-Job über eine zugehörige Sicherheitskonfiguration verfügt
- [CT.GLUE.PR.2] Erfordert eine AWS Glue-Sicherheitskonfiguration, um Daten in Amazon S3 S3-Zielen mithilfe von AWS KMS-Schlüsseln zu verschlüsseln
- [CT.KMS.PR.2] Erfordert, dass ein AWS KMS asymmetrischer Schlüssel mit RSA-Schlüsselmaterial, der für die Verschlüsselung verwendet wird, eine Schlüssellänge von mehr als 2048 Bit hat
- [CT.KMS.PR.3] Eine AWS KMS wichtige Richtlinie muss eine Erklärung enthalten, die die Gewährung von AWS KMS Zuschüssen auf Dienstleistungen beschränkt AWS
- [CT.LAMBDA.PR.4] Für die Gewährung des Zugriffs auf eine AWS Organisation oder ein bestimmtes AWS Konto ist eine AWS Lambda Ebenenberechtigung erforderlich
- [CT.LAMBDA.PR.5] Für die Verwendung der AWS IAM-basierten Authentifizierung ist eine AWS Lambda Funktions-URL erforderlich
- [CT.LAMBDA.PR.6] Erfordert eine CORS-Richtlinie für AWS Lambda Funktions-URLs, um den Zugriff auf bestimmte Ursprünge einzuschränken
- [CT.NEPTUNE.PR.4] Erfordert einen Amazon Neptune Neptune-DB-Cluster, um den CloudWatch Amazon-Protokollexport für Audit-Logs zu aktivieren
- [CT.NEPTUNE.PR.5] Für einen Amazon Neptune Neptune-DB-Cluster muss ein Aufbewahrungszeitraum für Backups festgelegt werden, der mindestens sieben Tage beträgt

- [CT.REDSHIFT.PR.9] Erfordert, dass eine Amazon Redshift Redshift-Cluster-Parametergruppe für die Verwendung von Secure Sockets Layer (SSL) für die Verschlüsselung von Daten bei der Übertragung konfiguriert ist

Diese neuen proaktiven Kontrollen sind im Handel erhältlich AWS-Regionen , wo auch AWS Control Tower erhältlich ist. Weitere Informationen zu diesen Kontrollen finden Sie unter Proaktive Kontrollen. Weitere Informationen darüber, wo die Kontrollen verfügbar sind, finden Sie unter Einschränkungen der Steuerung.

Neue Detektivsteuerungen

Der Security Hub Service-Managed Standard: AWS Control Tower wurde um neue Kontrollen erweitert. Diese Kontrollen helfen Ihnen dabei, Ihre Unternehmensführung zu verbessern. Sie agieren als Teil des Security Hub Service-Managed Standard: AWS Control Tower, nachdem Sie sie auf einer bestimmten Organisationseinheit aktiviert haben.

- [SH.Athena.1] Athena-Arbeitsgruppen sollten im Ruhezustand verschlüsselt sein
- [SH.Neptune.1] Neptune-DB-Cluster sollten im Ruhezustand verschlüsselt werden
- [SH.Neptune.2] Neptune-DB-Cluster sollten Audit-Logs in Logs veröffentlichen CloudWatch
- [SH.Neptune.3] Neptune DB-Cluster-Snapshots sollten nicht öffentlich sein
- [SH.Neptune.4] Bei Neptune-DB-Clustern sollte der Löschschutz aktiviert sein
- [SH.Neptune.5] Bei Neptune-DB-Clustern sollten automatische Backups aktiviert sein
- [SH.Neptune.6] Neptune DB-Cluster-Snapshots sollten im Ruhezustand verschlüsselt werden
- [SH.Neptune.7] Neptune-DB-Cluster sollten die IAM-Datenbankauthentifizierung aktiviert haben
- [SH.Neptune.8] Neptune-DB-Cluster sollten so konfiguriert sein, dass sie Tags in Snapshots kopieren
- [SH.RDS.27] RDS-DB-Cluster sollten im Ruhezustand verschlüsselt werden

Die neuen AWS Security Hub Detective Controls sind in den meisten Ländern verfügbar, in AWS-Regionen denen AWS Control Tower verfügbar ist. Weitere Informationen zu diesen Kontrollen finden Sie unter Kontrollen, die für den Service-Managed Standard gelten: AWS Control Tower. Weitere Informationen darüber, wo die Kontrollen verfügbar sind, finden Sie unterEinschränkungen der Kontrolle.

Es wurde ein neuer Drift-Typ gemeldet: Vertrauenswürdiger Zugriff deaktiviert

21. September 2023

(Für die AWS Control Tower Tower-Landezone ist kein Update erforderlich.)

Nachdem Sie Ihre AWS Control Tower-Landezone eingerichtet haben, können Sie den vertrauenswürdigen Zugriff auf AWS Control Tower in deaktivieren AWS Organizations. Dies führt jedoch zu Abweichungen.

Wenn der Drift-Typ Trusted Access deaktiviert ist, benachrichtigt Sie AWS Control Tower, wenn diese Art von Drift auftritt, sodass Sie Ihre AWS Control Tower Tower-Landezone reparieren können. Weitere Informationen finden Sie unter Arten von Abweichungen in der Unternehmensführung.

Vier weitere AWS-Regionen

13. September 2023

(Für die AWS Control Tower Tower-Landezone ist kein Update erforderlich.)

AWS Control Tower ist jetzt im asiatisch-pazifischen Raum (Hyderabad), Europa (Spanien und Zürich) und im Nahen Osten (VAE) verfügbar.

Wenn Sie AWS Control Tower bereits verwenden und die Governance-Funktionen in Ihren Konten auf diese Region ausweiten möchten, gehen Sie in Ihrem AWS Control Tower Tower-Dashboard zur Seite Einstellungen, wählen Sie die Region aus und aktualisieren Sie dann Ihre landing zone. Nach einem landing zone Zone-Update müssen Sie alle Konten aktualisieren, die von AWS Control Tower verwaltet werden, um Ihre Konten und Organisationseinheiten in der neuen Region unter Kontrolle zu bringen. Weitere Informationen finden Sie unter Über Updates.

Eine vollständige Liste der Regionen, in denen AWS Control Tower verfügbar ist, finden Sie in der AWS-Region Tabelle.

AWS Control Tower in der Region Tel Aviv verfügbar

28. August 2023

(Für die AWS Control Tower Tower-Landezone ist kein Update erforderlich.)

AWS Control Tower gibt die Verfügbarkeit in der Region Israel (Tel Aviv) bekannt.

Wenn Sie AWS Control Tower bereits verwenden und die Governance-Funktionen in Ihren Konten auf diese Region ausweiten möchten, gehen Sie in Ihrem AWS Control Tower Tower-Dashboard zur Seite Einstellungen, wählen Sie die Region aus und aktualisieren Sie dann Ihre landing zone. Nach einem landing zone Zone-Update müssen Sie alle Konten aktualisieren, die von AWS Control Tower verwaltet werden, um Ihre Konten und Organisationseinheiten in der neuen Region unter Kontrolle zu bringen. Weitere Informationen finden Sie unter Über Updates.

Eine vollständige Liste der Regionen, in denen AWS Control Tower verfügbar ist, finden Sie in der AWS-Region Tabelle.

AWS Control Tower führt 28 neue proaktive Kontrollen ein

24. Juli 2023

(Für die AWS Control Tower Tower-Landezone ist kein Update erforderlich.)

AWS Control Tower fügt 28 neue proaktive Kontrollen hinzu, um Sie bei der Verwaltung Ihrer AWS Umgebung zu unterstützen.

Proaktive Kontrollen verbessern die Governance-Funktionen von AWS Control Tower in Ihren AWS Umgebungen mit mehreren Konten, indem nicht konforme Ressourcen blockiert werden, bevor sie bereitgestellt werden. Diese Steuerelemente helfen bei der Verwaltung von AWS Diensten wie Amazon CloudWatch, Amazon Neptune ElastiCache AWS Step Functions, Amazon und Amazon DocumentDB. Die neuen Kontrollen helfen Ihnen dabei, Kontrollziele wie die Einrichtung von Protokollierung und Überwachung, die Verschlüsselung ruhender Daten oder die Verbesserung der Ausfallsicherheit zu erreichen.

Hier ist eine vollständige Liste der neuen Kontrollen:

- [CT.APPSYNC.PR.1] Erfordert eine AWS AppSync GraphQL-API, um die Protokollierung zu aktivieren
- [CT.CLOUDWATCH.PR.1] Für einen CloudWatch Amazon-Alarm muss eine Aktion für den Alarmstatus konfiguriert sein
- [CT.CLOUDWATCH.PR.2] Erfordern, dass eine CloudWatch Amazon-Protokollgruppe mindestens ein Jahr lang aufbewahrt wird
- [CT.CLOUDWATCH.PR.3] Erfordert, dass eine CloudWatch Amazon-Protokollgruppe im Ruhezustand mit einem KMS-Schlüssel verschlüsselt wird AWS

- [CT.CLOUDWATCH.PR.4] Erfordert die Aktivierung einer Amazon-Alarmaktion CloudWatch
- [CT.DOCUMENTDB.PR.1] Erfordert, dass ein Amazon DocumentDB-Cluster im Ruhezustand verschlüsselt wird
- [CT.DOCUMENTDB.PR.2] Für einen Amazon DocumentDB-Cluster müssen automatische Backups aktiviert sein
- [CT.DYNAMODB.PR.2] Erfordert, dass eine Amazon DynamoDB-Tabelle im Ruhezustand mithilfe von Schlüsseln verschlüsselt wird AWS KMS
- [CT.EC2.PR.13] Für eine Amazon EC2 EC2-Instance muss die detaillierte Überwachung aktiviert sein
- [CT.EKS.PR.1] Erfordert die Konfiguration eines Amazon EKS-Clusters mit deaktiviertem öffentlichen Zugriff auf den Cluster-Kubernetes-API-Serverendpunkt
- [CT.ELASTICACHE.PR.1] Für einen Amazon ElastiCache for Redis-Cluster müssen automatische Backups aktiviert sein
- [CT.ELASTICACHE.PR.2] Für einen Amazon ElastiCache for Redis-Cluster müssen automatische Upgrades für kleinere Versionen aktiviert sein
- [CT.ELASTICACHE.PR.3] Für eine Amazon ElastiCache for Redis-Replikationsgruppe muss der automatische Failover aktiviert sein
- [CT.ELASTICACHE.PR.4] Für eine ElastiCache Amazon-Replikationsgruppe muss die Verschlüsselung im Ruhezustand aktiviert sein
- [CT.ELASTICACHE.PR.5] Für eine Amazon ElastiCache for Redis-Replikationsgruppe muss die Verschlüsselung bei der Übertragung aktiviert sein
- [CT.ELASTICACHE.PR.6] Erfordert einen ElastiCache Amazon-Cache-Cluster, um eine benutzerdefinierte Subnetzgruppe zu verwenden
- [CT.ELASTICACHE.PR.7] Erfordert, dass eine ElastiCache Amazon-Replikationsgruppe früherer Redis-Versionen über die Redis-AUTH-Authentifizierung verfügt
- [CT.ELASTICBEANSTALK.PR.3] Für eine AWS Elastic Beanstalk Beanstalk-Umgebung ist eine Logging-Konfiguration erforderlich
- [CT.LAMBDA.PR.3] Eine AWS Lambda Funktion muss sich in einer vom Kunden verwalteten Amazon Virtual Private Cloud (VPC) befinden
- [CT.NEPTUNE.PR.1] Erfordert, dass ein Amazon Neptune Neptune-DB-Cluster über eine (IAM) - Datenbankauthentifizierung verfügt AWS Identity and Access Management
- [CT.NEPTUNE.PR.2] Für einen Amazon Neptune Neptune-DB-Cluster muss der Löschschutz aktiviert sein

- [CT.NEPTUNE.PR.3] Für einen Amazon Neptune Neptune-DB-Cluster muss die Speicherverschlüsselung aktiviert sein
- [CT.REDSHIFT.PR.8] Erfordert die Verschlüsselung eines Amazon Redshift Redshift-Clusters
- [CT.S3.PR.9] Erfordert, dass für einen Amazon S3 S3-Bucket S3 Object Lock aktiviert ist
- [CT.S3.PR.10] Für einen Amazon S3-Bucket muss die serverseitige Verschlüsselung mithilfe von Schlüsseln konfiguriert sein AWS KMS
- [CT.S3.PR.11] Für einen Amazon S3 S3-Bucket muss die Versionierung aktiviert sein
- [CT.STEPFUNCTIONS.PR.1] Erfordert, dass auf einer Zustandsmaschine die Protokollierung aktiviert ist AWS Step Functions
- [CT.STEPFUNCTIONS.PR.2] Erfordert, dass auf einer Zustandsmaschine die Ablaufverfolgung aktiviert ist AWS Step Functions AWS X-Ray

Proaktive Kontrollen in AWS Control Tower werden mithilfe von AWS CloudFormation Hooks implementiert, die nicht konforme Ressourcen identifizieren und blockieren, bevor sie bereitgestellt AWS CloudFormation werden. Proaktive Kontrollen ergänzen die bestehenden präventiven und detektiven Kontrollfunktionen in AWS Control Tower.

Diese neuen proaktiven Kontrollen sind überall verfügbar AWS-Regionen , wo AWS Control Tower verfügbar ist. Weitere Informationen zu diesen Kontrollen finden Sie unter Proaktive Kontrollen.

AWS Control Tower lehnt zwei Kontrollen ab

18. Juli 2023

(Für die AWS Control Tower Tower-Landezone ist kein Update erforderlich.)

AWS Control Tower führt regelmäßige Überprüfungen seiner Sicherheitskontrollen durch, um sicherzustellen, dass sie auf dem neuesten Stand sind und weiterhin als bewährte Methoden gelten. Die folgenden beiden Kontrollen sind seit dem 18. Juli 2023 veraltet und werden mit Wirkung zum 18. August 2023 aus der Kontrollbibliothek entfernt. Sie können diese Steuerungen für keine Organisationseinheiten mehr aktivieren. Sie können sich dafür entscheiden, diese Steuerungen vor dem Entfernungsdatum zu deaktivieren.

- [SH.S3.4] Bei S3-Buckets sollte die serverseitige Verschlüsselung aktiviert sein
- [CT.S3.PR.7] Für einen Amazon S3-Bucket muss die serverseitige Verschlüsselung konfiguriert sein

Grund für die Vernachlässigung

Ab Januar 2023 konfigurierte Amazon S3 die Standardverschlüsselung für alle neuen und vorhandenen unverschlüsselten Buckets, um serverseitige Verschlüsselung mit verwalteten S3-Schlüsseln (SSE-S3) als Basisverschlüsselungsebene für neue Objekte anzuwenden, die in diese Buckets hochgeladen wurden. Es wurden keine Änderungen an der Standardverschlüsselungskonfiguration für einen vorhandenen Bucket vorgenommen, für den bereits SSE-S3 oder serverseitige Verschlüsselung mit AWS Key Management Service (KMS) -Schlüsseln (SSE-KMS) konfiguriert war.AWS

AWS-Control-Tower-Landezone, Version 3.2

16. Juni 2023

(Für die AWS Control Tower landing zone ist ein Update auf Version 3.2 erforderlich. Weitere Informationen finden Sie unterAktualisieren Ihrer Landing Zone).

Mit Version 3.2 der AWS Control Tower landing zone sind die Kontrollen, die Teil des AWS Security Hub Service-Managed Standard: AWS Control Tower sind, jetzt allgemein verfügbar. Es bietet die Möglichkeit, den Drift-Status von Kontrollen, die Teil dieses Standards sind, in der AWS Control Tower-Konsole einzusehen.

Dieses Update beinhaltet eine neue serviceverknüpfte Rolle (SLR), die. AWSServiceRoleForAWSControlTower Diese Rolle unterstützt AWS Control Tower bei der Erstellung einer EventBridge verwalteten Regel, die AWSControlTowerManagedRulein jedem Mitgliedskonto so genannt wird. Diese verwaltete Regel sammelt AWS Security Hub Findereignisse, anhand derer mithilfe von AWS Control Tower Kontrollabweichungen festgestellt werden können.

Diese Regel ist die erste verwaltete Regel, die von AWS Control Tower erstellt wurde. Die Regel wird nicht von einem Stack bereitgestellt, sondern 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 Service Principal angezeigt.

Zuvor hatte AWS Control Tower die AWSControlTowerExecutionRolle übernommen, Operationen in Mitgliedskonten durchzuführen. Diese neue Rolle und Regel entsprechen besser dem Best-Practice-Prinzip, bei der Ausführung von Vorgängen in einer AWS Umgebung mit mehreren Konten die geringsten Rechte zuzulassen. Die neue Rolle bietet spezielle Berechtigungen, die 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 enthält auch eine neue StackSet Ressource im VerwaltungskontoBP_BASELINE_SERVICE_LINKED_ROLE, mit der zunächst die dienstverknüpfte Rolle bereitgestellt wird.

Wenn eine Abweichung der Security Hub-Kontrolle gemeldet wird (in der landing zone 3.2 und höher), erhält AWS Control Tower täglich ein Status-Update von Security Hub. Obwohl die Kontrollen in jeder kontrollierten Region aktiv sind, sendet AWS Control Tower die AWS Security Hub Finding-Ereignisse nur an die AWS Control Tower Tower-Heimatregion. Weitere Informationen finden Sie unter Berichterstattung über Kontrollabweichungen in Security Hub.

Update zur Steuerung „Region Deny“

Diese landing zone Zone-Version beinhaltet auch ein Update für die Steuerung „Region Deny“.

Globale Dienste und APIs hinzugefügt

- AWS Billing and Cost Management (`billing:*`)
- AWS CloudTrail (`cloudtrail:LookupEvents`) um die Sichtbarkeit globaler Ereignisse in den Mitgliedskonten zu ermöglichen.
- AWS Konsolidierte Abrechnung (`consolidatedbilling:*`)
- AWS Mobile Anwendung der 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 entferntS3:`GetAccountPublic`, weil es sich nicht um eine gültige Aktion handelt.
- Wurde entferntS3:`PutAccountPublic`, weil es sich nicht um eine gültige Aktion handelt.

AWS Control Tower verwaltet Konten auf der Grundlage von IDs

14. Juni 2023

(Für die AWS Control Tower Tower-Landezone ist kein Update erforderlich.)

AWS Control Tower erstellt und verwaltet jetzt Konten, die Sie in Account Factory erstellen, indem die AWS Konto-ID und nicht die E-Mail-Adresse des Kontos verfolgt wird.

Bei der Bereitstellung eines Kontos muss der Kontoanforderer immer über die `CreateAccount` und die `DescribeCreateAccountStatus` entsprechenden Berechtigungen verfügen. Dieser Berechtigungssatz ist Teil der Administratorrolle und wird automatisch vergeben, wenn ein Anforderer die Administratorrolle übernimmt. Wenn Sie die Erlaubnis zur Bereitstellung von Konten delegieren, müssen Sie diese Berechtigungen möglicherweise direkt für die Kontoanforderer hinzufügen.

Zusätzliche Security Hub Hub-Detektivkontrollen sind in der AWS Control Tower Tower-Steuerungsbibliothek verfügbar

12. Juni 2023

(Für die AWS Control Tower Tower-Landezone ist kein Update erforderlich.)

AWS Control Tower hat der Kontrollbibliothek von AWS Control Tower zehn neue AWS Security Hub Detective Controls hinzugefügt. Diese neuen Kontrollen zielen auf Dienste wie API Gateway AWS CodeBuild, Amazon Elastic Compute Cloud (EC2), Amazon Elastic Load Balancer, Amazon Redshift, Amazon SageMaker und ab. AWS WAF Diese neuen Kontrollen helfen Ihnen dabei, Ihre Governance-Position zu verbessern, indem sie Kontrollziele wie die Einrichtung von Protokollierung und Überwachung, die Beschränkung des Netzwerkzugriffs und die Verschlüsselung von Daten im Ruhezustand erfüllen.

Diese Kontrollen sind Teil des Security Hub Service-Managed Standard: AWS Control Tower, nachdem Sie sie auf einer bestimmten Organisationseinheit aktiviert haben.

- [sh.Account.1] Sicherheitskontaktinformationen sollten bereitgestellt werden für AWS-Konto
- [sh.APIGateway.8] API Gateway Gateway-Routen sollten einen Autorisierungstyp angeben
- [sh.ApiGateway.9] Die Zugriffsprotokollierung sollte für API Gateway V2 Stages konfiguriert sein
- [SH. CodeBuild.3] CodeBuild S3-Protokolle sollten verschlüsselt sein
- [SH.EC2.25] EC2-Startvorlagen sollten Netzwerkschnittstellen keine öffentlichen IPs zuweisen

- [SH.ELB.1] Application Load Balancer sollte so konfiguriert sein, dass alle HTTP-Anfragen an HTTPS umgeleitet werden
- [sh.RedShift.10] Redshift-Cluster sollten im Ruhezustand verschlüsselt werden
- [SH. SageMaker.2] SageMaker Notebook-Instances sollten in einer benutzerdefinierten VPC gestartet werden
- [SH. SageMaker.3] Benutzer sollten keinen Root-Zugriff auf SageMaker Notebook-Instanzen haben
- [SH.WAF.10] Eine WAFV2-Web-ACL sollte mindestens eine Regel oder Regelgruppe haben

Die neuen AWS Security Hub Detective Controls sind überall verfügbar AWS-Regionen , wo AWS Control Tower verfügbar ist. Weitere Informationen zu diesen Kontrollen finden Sie unter Kontrollen, die für den Service-Managed Standard gelten: AWS Control Tower.

AWS Control Tower veröffentlicht Tabellen mit Kontrollmetadaten

7. Juni 2023

(Für die AWS Control Tower Tower-Landezone ist kein Update erforderlich.)

AWS Control Tower bietet jetzt vollständige Tabellen mit Kontrollmetadaten als Teil der veröffentlichten Dokumentation. Wenn Sie mit den Kontroll-APIs arbeiten, können Sie den API-ControlIdentifier jedes Steuerelements nachschlagen, bei dem es sich um einen eindeutigen ARN handelt, der jedem Steuerelement zugeordnet ist. AWS-Region Die Tabellen enthalten die Rahmenbedingungen und Kontrollziele, die jede Kontrolle abdeckt. Bisher waren diese Informationen nur in der Konsole verfügbar.

Die Tabellen enthalten auch die Metadaten für Security Hub-Steuerelemente, die Teil des AWS Security Hub Service-Managed Standard:AWS Control Tower sind. Vollständige Informationen finden Sie unter Tabellen mit Kontrollmetadaten.

Eine verkürzte Liste von Kontrollbezeichnern und einige Anwendungsbeispiele finden Sie unter Ressourcen-Identifikatoren für APIs und Steuerelemente.

Terraform-Unterstützung für Account Factory Customization

6. Juni 2023

(Für die AWS Control Tower Tower-Landezone ist kein Update erforderlich.)

AWS Control Tower bietet über Account Factory Customization (AFC) Support für eine einzelne Region für Terraform. Ab dieser Version können Sie AWS Control Tower und Service Catalog zusammen verwenden, um AFC-Konto-Blueprints in Terraform Open Source zu definieren. Sie können Ihre neuen und vorhandenen Ressourcen anpassen AWS-Konten, bevor Sie Ressourcen in AWS Control Tower bereitstellen. Standardmäßig können Sie mit dieser Funktion Konten mit Terraform in Ihrer AWS Control Tower Tower-Heimatregion bereitstellen und aktualisieren.

Ein Konto-Blueprint beschreibt die spezifischen Ressourcen und Konfigurationen, die bei der Bereitstellung eines AWS-Konto Kontos erforderlich sind. Sie können den Blueprint als Vorlage verwenden, um mehrere AWS-Konten Blueprints in großem Maßstab zu erstellen.

Verwenden Sie zunächst die Terraform Reference Engine auf. GitHub Die Reference Engine konfiguriert den Code und die Infrastruktur, die erforderlich sind, damit die Terraform Open Source Engine mit Service Catalog funktioniert. Dieser einmalige Einrichtungsvorgang dauert einige Minuten. Danach können Sie Ihre benutzerdefinierten Kontoanforderungen in Terraform definieren und dann Ihre Konten mit dem genau definierten AWS Control Tower Account Factory-Workflow bereitstellen. Kunden, die lieber mit Terraform arbeiten, können die AWS Control Tower Tower-Kontoanpassung mit AFC in großem Umfang nutzen und erhalten nach der Bereitstellung sofort Zugriff auf jedes Konto.

Informationen zum Erstellen dieser Anpassungen finden Sie unter Produkte erstellen und Erste Schritte mit Terraform Open Source in der Service Catalog-Dokumentation. Diese Funktion ist überall verfügbar AWS-Regionen , wo AWS Control Tower verfügbar ist.

AWS IAM Identity Center-Selbstmanagement für die landing zone verfügbar

6. Juni 2023

(Für die AWS Control Tower Tower-Landezone ist kein Update erforderlich.)

AWS Control Tower unterstützt jetzt eine optionale Auswahl eines Identitätsanbieters für eine AWS Control Tower Tower-Landezone, die Sie während der Einrichtung oder Aktualisierung konfigurieren können. Standardmäßig ist die landing zone für die Verwendung von AWS IAM Identity Center aktiviert. Dies entspricht den unter Organizing Your AWS Environment Using Multiple Accounts definierten Best-Practices-Richtlinien. Sie haben jetzt drei Alternativen:

- Sie können die Standardeinstellung akzeptieren und AWS Control Tower erlauben, AWS IAM Identity Center für Sie einzurichten und zu verwalten.
- Sie können sich dafür entscheiden, das AWS IAM Identity Center selbst zu verwalten, um Ihren spezifischen Geschäftsanforderungen gerecht zu werden.

- Sie können optional einen externen Identitätsanbieter hinzuziehen und diesen selbst verwalten, indem Sie ihn bei Bedarf über das IAM Identity Center verbinden. Sie sollten die Option eines Identitätsanbieters verwenden, wenn Ihr regulatorisches Umfeld die Verwendung eines bestimmten Anbieters erfordert oder wenn Sie in einem Land tätig sind, in AWS-Regionen dem AWS IAM Identity Center nicht verfügbar ist.

Weitere Informationen finden Sie unter Anleitung zum IAM Identity Center.

Die Auswahl von Identitätsanbietern auf Kontoebene wird nicht unterstützt. Diese Funktion gilt nur für die gesamte landing zone. Die Option eines AWS Control Tower-Identitätsanbieters ist überall verfügbar AWS-Regionen , wo AWS Control Tower verfügbar ist.

AWS Control Tower befasst sich mit gemischter Governance für Organisationseinheiten

1. Juni 2023

(Für die AWS Control Tower Tower-Landezone ist kein Update erforderlich.)

Mit dieser Version verhindert AWS Control Tower, dass Kontrollen in einer Organisationseinheit (OU) bereitgestellt werden, wenn sich diese OU in einem gemischten Governance-Status befindet. Eine gemischte Governance tritt in einer Organisationseinheit auf, wenn Konten nicht aktualisiert werden, nachdem AWS Control Tower die Governance auf eine neue AWS-Region erweitert oder die Governance aufgehoben hat. Diese Version hilft Ihnen dabei, die Einhaltung einheitlicher Vorschriften für die Mitgliedskonten dieser Organisationseinheit zu gewährleisten. Weitere Informationen finden Sie unter Vermeiden Sie gemischte Verwaltungsstrukturen bei der Konfiguration von Regionen.

Zusätzliche proaktive Kontrollen verfügbar

19. Mai 2023

(Für die AWS Control Tower Tower-Landezone ist kein Update erforderlich.)

AWS Control Tower fügt 28 neue proaktive Kontrollen hinzu, die Sie bei der Verwaltung Ihrer Umgebung mit mehreren Konten und der Erfüllung bestimmter Kontrollziele unterstützen, wie z. B. Datenverschlüsselung im Ruhezustand oder Beschränkung des Netzwerkzugriffs. Proaktive Kontrollen werden mit AWS CloudFormation Hooks implementiert, die Ihre Ressourcen überprüfen, bevor sie bereitgestellt werden. Die neuen Kontrollen können dabei helfen, AWS Dienste wie Amazon

OpenSearch Service, Amazon EC2 Auto Scaling, Amazon SageMaker, Amazon API Gateway und Amazon Relational Database Service (RDS) zu steuern.

Proaktive Kontrollen werden in allen Geschäften unterstützt AWS-Regionen , in denen AWS Control Tower verfügbar ist.

OpenSearch Amazon-Dienst

- [CT.OPENSEARCH.PR.1] Sie benötigen eine Elasticsearch-Domain, um Daten im Ruhezustand zu verschlüsseln
- [CT.OPENSEARCH.PR.2] Erfordert, dass eine Elasticsearch-Domain in einer benutzerdefinierten Amazon-VPC erstellt wird
- [CT.OPENSEARCH.PR.3] Erfordert eine Elasticsearch-Domain, um zwischen Knoten gesendete Daten zu verschlüsseln
- [CT.OPENSEARCH.PR.4] Erfordert eine Elasticsearch-Domain, um Fehlerprotokolle an Amazon Logs zu senden CloudWatch
- [CT.OPENSEARCH.PR.5] Erfordert eine Elasticsearch-Domain, um Audit-Logs an Amazon Logs zu senden CloudWatch
- [CT.OPENSEARCH.PR.6] Eine Elasticsearch-Domain muss über Zonenerkennung und mindestens drei Datenknoten verfügen
- [CT.OPENSEARCH.PR.7] Erfordert, dass eine Elasticsearch-Domain über mindestens drei dedizierte Master-Knoten verfügt
- [CT.OPENSEARCH.PR.8] Für die Verwendung von TLSv1.2 ist eine Elasticsearch Service-Domain erforderlich
- [CT.OPENSEARCH.PR.9] Erfordert eine Amazon OpenSearch Service-Domain, um Daten im Ruhezustand zu verschlüsseln
- [CT.OPENSEARCH.PR.10] Erfordert, dass eine Amazon OpenSearch Service-Domain in einer benutzerdefinierten Amazon VPC erstellt wird
- [CT.OPENSEARCH.PR.11] Erfordert eine Amazon OpenSearch Service-Domain, um zwischen Knoten gesendete Daten zu verschlüsseln
- [CT.OPENSEARCH.PR.12] Erfordert eine Amazon OpenSearch Service-Domain, um Fehlerprotokolle an Amazon Logs zu senden CloudWatch
- [CT.OPENSEARCH.PR.13] Erfordert eine Amazon OpenSearch Service-Domain, um Audit-Logs an Amazon Logs zu senden CloudWatch

- [CT.OPENSEARCH.PR.14] Erfordert, dass eine Amazon OpenSearch Service-Domain über Zone Awareness und mindestens drei Datenknoten verfügt
- [CT.OPENSEARCH.PR.15] Erfordert eine Amazon OpenSearch Service-Domain, um eine differenzierte Zugriffskontrolle zu verwenden
- [CT.OPENSEARCH.PR.16] Für die Verwendung von TLSv1.2 ist eine Amazon Service-Domain erforderlich OpenSearch

Amazon EC2 Auto Scaling

- [CT.AUTOSCALING.PR.1] Eine Amazon EC2 Auto Scaling Scaling-Gruppe muss über mehrere Availability Zones verfügen
- [CT.AUTOSCALING.PR.2] Erfordert eine Amazon EC2 Auto Scaling Scaling-Gruppenstartkonfiguration, um Amazon EC2 EC2-Instances für IMDSv2 zu konfigurieren
- [CT.AUTOSCALING.PR.3] Eine Amazon EC2 Auto Scaling Scaling-Startkonfiguration erfordert ein Antwortlimit für Single-Hop-Metadaten
- [CT.AUTOSCALING.PR.4] Für eine Amazon EC2 Auto Scaling-Gruppe, die einem Amazon Elastic Load Balancing (ELB) zugeordnet ist, müssen ELB-Zustandsprüfungen aktiviert sein
- [CT.AUTOSCALING.PR.5] Erfordern, dass eine Amazon EC2 Auto Scaling Scaling-Gruppenstartkonfiguration keine Amazon EC2 EC2-Instances mit öffentlichen IP-Adressen hat
- [CT.AUTOSCALING.PR.6] Erfordern, dass alle Amazon EC2 Auto Scaling Scaling-Gruppen mehrere Instance-Typen verwenden
- [CT.AUTOSCALING.PR.8] Erfordert, dass eine Amazon EC2 Auto Scaling Scaling-Gruppe EC2-Startvorlagen konfiguriert hat

Amazon SageMaker

- [CT.SAGEMAKER.PR.1] Erfordert eine SageMaker Amazon-Notebook-Instance, um direkten Internetzugang zu verhindern
- [CT.SAGEMAKER.PR.2] Erfordert, dass SageMaker Amazon-Notebook-Instances in einer benutzerdefinierten Amazon VPC bereitgestellt werden
- [CT.SAGEMAKER.PR.3] Erfordert, dass Amazon SageMaker Amazon-Notebook-Instances der Root-Zugriff verweigert wird

Amazon API Gateway

- [CT.APIGATEWAY.PR.5] Erfordert Amazon API Gateway V2 Websocket- und HTTP-Routen, um einen Autorisierungstyp anzugeben

Amazon Relational Database Service (RDS)

- [CT.RDS.PR.25] Für einen Amazon RDS-Datenbankcluster muss die Protokollierung konfiguriert sein

Weitere Informationen finden Sie unter Proaktive Kontrollen.

Aktualisierte proaktive Amazon EC2 EC2-Kontrollen

2. Mai 2023

(Für die AWS Control Tower Tower-Landezone ist kein Update erforderlich.)

AWS Control Tower hat zwei proaktive Kontrollen aktualisiert: CT.EC2.PR.3 undCT.EC2.PR.4.

Bei der aktualisierten CT.EC2.PR.3 Steuerung wird jede AWS CloudFormation Bereitstellung, die auf eine Präfixliste für eine Sicherheitsgruppenressource verweist, für die Bereitstellung gesperrt, es sei denn, sie bezieht sich auf Port 80 oder 443.

Für das aktualisierte CT.EC2.PR.4 Steuerelement wird jede AWS CloudFormation Bereitstellung, die auf eine Präfixliste für eine Sicherheitsgruppenressource verweist, blockiert, wenn der Port 3389, 20, 23, 110, 143, 3306, 8080, 1433, 9200, 9300, 25, 445, 135, 21, 1434, 4333, 5432, 5500, 5601, 22, 3000, 5000, 8088, 8888 lautet.

AWS-Regionen Sieben weitere verfügbar

19. April 2023

(Für die AWS Control Tower Tower-Landezone ist kein Update erforderlich.)

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). Diese zusätzlichen Regionen für AWS Control Tower, sogenannte Opt-in-Regionen, sind standardmäßig nicht aktiv, mit Ausnahme der Region USA West (Nordkalifornien), die standardmäßig aktiv ist.

Einige Kontrollen in AWS Control Tower funktionieren in einigen dieser zusätzlichen Bereiche, in AWS-Regionen denen AWS Control Tower verfügbar ist, nicht, da diese Regionen die erforderlichen Basisfunktionen nicht unterstützen. Details hierzu finden Sie unter Einschränkungen der Kontrolle.

Unter diesen neuen Regionen ist cFCT im asiatisch-pazifischen Raum (Jakarta und Osaka) nicht verfügbar. Die Verfügbarkeit in anderen Ländern AWS-Regionen ist unverändert.

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

Die von AFT benötigten vPCe-Endpunkte sind in der Region Naher Osten (Bahrain) nicht verfügbar. Kunden, die AFT in dieser Region einsetzen, müssen die Bereitstellung mit dem Parameter durchführen. `aft_vpc_endpoints=false` Weitere Informationen finden Sie in dem Parameter in der README-Datei.

AWS Control Tower VPCs haben aufgrund einer Beschränkung in Amazon EC2 zwei Availability Zones in der Region USA West (Nordkalifornien). `us-west-1` In den USA West (Nordkalifornien) sind sechs Subnetze auf zwei Availability Zones aufgeteilt. Weitere Informationen finden Sie unter Überblick über AWS Control Tower und VPCs.

AWS Control Tower hat neue Berechtigungen hinzugefügt`AWSControlTowerServiceRolePolicy`, die es AWS Control Tower ermöglichen`EnableRegion`, Aufrufe an die vom AWS Account Management Service implementierten `GetRegionOptStatus` API`ListRegions`, und zu tätigen, um diese zusätzlich für Ihre gemeinsamen Konten in der landing zone (Verwaltungskonto, Protokollarchivkonto, Auditkonto) und Ihre OU-Mitgliedskonten AWS-Regionen verfügbar zu machen. Weitere Informationen finden Sie unter Verwaltete Richtlinien für AWS Control Tower.

Rückverfolgung von Anfragen zur Kontoanpassung von Account Factory for Terraform (AFT)

16. Februar 2023

AFT unterstützt die Rückverfolgung von Anfragen zur Kontoanpassung. Jedes Mal, wenn Sie eine Anfrage zur Kontoanpassung einreichen, generiert AFT ein eindeutiges Ablaufverfolgungstoken, das einen AWS Step Functions AFT-Anpassungsstatuscomputer durchläuft, der das Token im Rahmen seiner Ausführung protokolliert. Sie können 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. Weitere Informationen zu AFT finden Sie unter Überblick über AWS Control Tower Account Factory for Terraform. 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 AWS Step Functions Developer Guide

AWS-Control-Tower-Landezone, Version 3.1

9. Februar 2023

(Für die AWS Control Tower landing zone ist ein Update auf Version 3.1 erforderlich. Weitere Informationen finden Sie unterAktualisieren Ihrer Landing Zone)

Die AWS Control Tower landing zone Version 3.1 beinhaltet die folgenden Updates:

- Mit dieser Version deaktiviert AWS Control Tower die unnötige Zugriffsprotokollierung für Ihren Access Logging Bucket, den Amazon S3 S3-Bucket, in dem Zugriffsprotokolle im Log Archive-Konto gespeichert werden, während die Serverzugriffsprotokollierung für S3-Buckets weiterhin aktiviert wird. Diese Version enthält auch Aktualisierungen der Steuerung „Region Deny“, die zusätzliche Aktionen für globale Dienste wie AWS Support Pläne und ermöglichen. AWS Artifact
- Die Deaktivierung der Serverzugriffsprotokollierung für den Access Logging Bucket von AWS Control Tower veranlasst Security Hub, einen Befund für den Access Logging Bucket des Log-Archive-Kontos zu erstellen. Aufgrund einer AWS Security Hub Regel sollte die [S3.9] S3-Bucket-Serverzugriffsprotokollierung aktiviert sein. In Übereinstimmung mit Security Hub empfehlen wir, dass Sie dieses spezielle Ergebnis unterdrücken, wie in der Security Hub Hub-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 Protokolleinträge im Access-Logging-Bucket aufgezeichnet. Weitere Informationen zur Zugriffsprotokollierung finden Sie unter Protokollierung von Anfragen mithilfe der Serverzugriffsprotokollierung in der Amazon S3 S3-Dokumentation.
- Wir haben die Steuerung „Region Deny“ aktualisiert. Dieses Update ermöglicht Aktionen durch mehr globale Dienste. Einzelheiten zu diesem SCP finden Sie unter Zugriff verweigern auf AWS Grundlage der angeforderten Daten AWS-Region und unter Kontrollen, die den Schutz der Datenspeicherung verbessern.

Globale Dienste wurden hinzugefügt:

- AWS Account Management (`account:*`)
- AWS Aktivieren (`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 Lightsail () `lightsail:Get*`
- AWS Ressourcen Explorer (`resource-explorer-2:*`)
- Amazon S3 (`s3:CreateMultiRegionAccessPoint`,`s3:GetBucketPolicyStatus`,`s3:PutMultiRegionAcc`
- AWS Savings Plans (`savingsplans:*`)
- IAM-Identitätszentrum () `sso:*`
- AWS Support App (`supportapp:*`)
- AWS Support Pläne () `supportplans:*`
- AWS Nachhaltigkeit (`sustainability:*`)
- AWS Resource Groups Tagging API (`tag:GetResources`)
- AWS Marketplace Einblicke von Anbietern (`vendor-insights:ListEntitledSecurityProfiles`)

Proaktive Kontrollen sind allgemein verfügbar

24. Januar 2023

(Für die AWS Control Tower Tower-Landezone ist kein Update erforderlich.)

Optionale proaktive Kontrollen, die bereits in der Vorschauversion angekündigt wurden, sind jetzt allgemein verfügbar. Diese Kontrollen werden als proaktiv bezeichnet, da sie Ihre Ressourcen —

bevor die Ressourcen bereitgestellt werden — daraufhin überprüfen, ob die neuen Ressourcen den in Ihrer Umgebung aktivierten Kontrollen entsprechen. Weitere Informationen finden Sie unter Umfassende Kontrollen helfen bei der Bereitstellung und AWS Verwaltung von Ressourcen.

Januar — Dezember 2022

Im Jahr 2022 veröffentlichte AWS Control Tower die folgenden Updates:

- Gleichzeitige Kontooperationen
- Anpassung Account Factory (AFC)
- Umfassende Kontrollen helfen bei der Bereitstellung und AWS Verwaltung von Ressourcen
- Der Compliance-Status ist für alle AWS Config Regeln einsehbar
- API für Kontrollen und eine neue AWS CloudFormation Ressource
- cFCT unterstützt das Löschen von Stack-Sets
- Benutzerdefinierte Aufbewahrung von Protokollen
- Reparatur von Role Drift verfügbar
- AWS-Control-Tower-Landezone, Version 3.0
- Auf der Organisationsseite werden Ansichten von Organisationseinheiten und Konten zusammengefasst
- Einfachere Registrierung und Aktualisierung für einzelne Mitgliedskonten
- AFT unterstützt automatisierte Anpassungen für gemeinsam genutzte AWS Control Tower Tower-Konten
- Gleichzeitige Operationen für alle optionalen Steuerelemente
- Bestehende Sicherheits- und Protokollierungskonten
- AWS-Control-Tower-Landezone, Version 2.9
- AWS-Control-Tower-Landezone, Version 2.8

Gleichzeitige Kontooperationen

16. Dezember 2022

(Für die AWS Control Tower 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 bis zu fünf Aktionen

nacheinander ein und sehen Sie sich den Abschlussstatus jeder Anfrage an, während Ihre Konten im Hintergrund fertig aufgebaut werden. Sie müssen beispielsweise nicht mehr warten, bis jeder Vorgang abgeschlossen ist, bevor Sie ein anderes Konto aktualisieren oder bevor Sie eine gesamte Organisationseinheit (OU) erneut registrieren.

Anpassung Account Factory (AFC)

28. November 2022

(Für die AWS Control Tower Tower-Landezone ist kein Update erforderlich.)

Die werkseitige Anpassung von Konten ermöglicht es Ihnen, neue und bestehende Konten von der AWS Control Tower Tower-Konsole aus anzupassen. Diese neuen Anpassungsfunktionen bieten Ihnen die Flexibilität, Konto-Blueprints zu definieren. Dabei handelt es sich um AWS CloudFormation Vorlagen, die in einem speziellen Service Catalog-Produkt enthalten sind. Blueprints stellen vollständig angepasste Ressourcen und Konfigurationen bereit. Sie können sich auch dafür entscheiden, vordefinierte Blueprints zu verwenden, die von AWS Partnern erstellt und verwaltet werden und Ihnen helfen, Konten für bestimmte Anwendungsfälle anzupassen.

Bisher unterstützte AWS Control Tower Account Factory die Kontoanpassung in der Konsole nicht. Mit diesem Update von Account Factory können Sie Kontoanforderungen vordefinieren und diese 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 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 Ihr Konto mit der Erstellung fertig 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 Bibliothek „ AWS Erste Schritte“ auswählen. Weitere Informationen finden Sie unter Passen Sie Konten mit Account Factory Customization (AFC) an.

Umfassende Kontrollen helfen bei der Bereitstellung und AWS Verwaltung von Ressourcen

28. November 2022

(Für die AWS Control Tower Tower-Landezone ist kein Update erforderlich.)

AWS Control Tower unterstützt jetzt ein umfassendes Kontrollmanagement, einschließlich neuer, optionaler proaktiver Kontrollen, die über AWS CloudFormation Hooks implementiert werden. Diese Kontrollen werden als proaktiv bezeichnet, da sie Ihre Ressourcen — bevor die Ressourcen bereitgestellt werden — daraufhin überprüfen, ob die neuen Ressourcen den in Ihrer Umgebung aktivierten Kontrollen entsprechen.

Über 130 neue proaktive Kontrollen unterstützen Sie bei der Erfüllung bestimmter Richtlinienziele für Ihre AWS Control Tower Tower-Umgebung, bei der Erfüllung der Anforderungen branchenüblicher Compliance-Frameworks und bei der Steuerung von AWS Control Tower Tower-Interaktionen mit mehr als zwanzig anderen AWS Services.

Die Kontrollbibliothek von AWS Control Tower klassifiziert diese Kontrollen nach den zugehörigen AWS Services und Ressourcen. Weitere Informationen finden Sie unter Proaktive Kontrollen.

Mit dieser Version ist AWS Control Tower über den neuen Security Hub Service-Managed Standard auch in AWS Control Tower integriert, der den Standard AWS Foundational Security Best Practices (FSBP) unterstützt. AWS Security Hub In der Konsole können Sie neben den AWS Control Tower Tower-Kontrollen mehr als 160 Security Hub-Steuerelemente anzeigen und einen Security Hub-Sicherheitswert für Ihre AWS Control Tower Tower-Umgebung abrufen. Weitere Informationen finden Sie unter Security Hub-Steuerelemente.

Der Compliance-Status ist für alle AWS Config Regeln einsehbar

18. November 2022

(Für die AWS Control Tower Tower-Landezone ist kein Update erforderlich.)

AWS Control Tower zeigt jetzt den Compliance-Status 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, die sich auf Ihre Konten in AWS Control Tower auswirken, ob registriert oder nicht registriert, einsehen, ohne die AWS Control Tower Tower-Konsole verlassen zu müssen. Kunden können wählen, ob sie Config-Regeln, sogenannte Detective Controls, in AWS Control Tower oder direkt über den AWS Config Service einrichten möchten. Die von bereitgestellten Regeln AWS Config werden zusammen mit den von AWS Control Tower bereitgestellten Regeln angezeigt.

Bisher waren AWS Config Regeln, die über den AWS Config Service bereitgestellt wurden, in der AWS Control Tower Tower-Konsole nicht sichtbar. Kunden mussten zum AWS Config Service

navigieren, um AWS Config Regeln zu identifizieren, die den Anforderungen nicht entsprachen. Jetzt können Sie jede nicht konforme AWS Config Regel in der AWS Control Tower Tower-Konsole identifizieren. Um den Compliance-Status all Ihrer Config-Regeln einzusehen, navigieren Sie zur Seite mit den Kontodetails in der AWS Control Tower Tower-Konsole. Sie sehen eine Liste mit dem Compliance-Status der von AWS Control Tower verwalteten Kontrollen und den Konfigurationsregeln, die außerhalb von AWS Control Tower bereitgestellt werden.

API für Kontrollen und eine neue AWS CloudFormation Ressource

1. September 2022

(Für die AWS Control Tower 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 AWS CloudFormation Ressource unterstützt die API-Funktionalität für Steuerungen. Weitere Informationen finden Sie unter Automatisieren Sie Aufgaben in AWS Control Tower und AWS Control Tower Ressourcen erstellen mit AWS CloudFormation.

Mit diesen APIs können Sie Steuerungen in der AWS Control Tower Tower-Bibliothek aktivieren, deaktivieren und deren Anwendungsstatus anzeigen. Die APIs bieten Unterstützung für AWS CloudFormation, sodass Sie AWS Ressourcen als infrastructure-as-code (IaC) verwalten können. AWS Control Tower bietet optionale präventive und detektive Kontrollen, die Ihre politischen Absichten in Bezug auf eine gesamte Organisationseinheit (OU) und jedes AWS Konto innerhalb der OU zum Ausdruck bringen. 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 deaktiviert ein Steuerelement. Es startet einen asynchronen Vorgang, bei dem AWS Ressourcen in der angegebenen Organisationseinheit und den darin enthaltenen Konten gelöscht werden.
- GetControlOperation— Gibt den Status einer bestimmten EnableControlDisableControlOR-Operation zurück.
- ListEnabledControls— Listet die von AWS Control Tower für die angegebene Organisationseinheit aktivierten Kontrollen und die darin enthaltenen Konten auf.

Eine Liste der Kontrollnamen für optionale Kontrollen finden Sie unter Resource Identifiers for APIs and Controls im AWS Control Tower Tower-Benutzerhandbuch.

cFCT unterstützt das Löschen von Stack-Sets

26. August 2022

(Für die AWS Control Tower 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 zunächst den Wert `enable_stack_set_deletion` auf festlegen`true`, werden beim nächsten Aufruf von cFCt ALLE Ressourcen, die mit dem Präfix beginnen`CustomControlTower-`, die über das zugehörige Schlüssel-Tag `Key:AWS_Solutions, Value: CustomControlTowerStackSet` verfügen und die nicht in der Manifestdatei deklariert sind, zum Löschen zwischengespeichert.

Benutzerdefinierte Aufbewahrung von Protokollen

15. August 2022

(Update für die AWS Control Tower Tower-Landezone erforderlich. Weitere Informationen finden Sie unterAktualisieren Ihrer Landing Zone)

AWS Control Tower bietet jetzt die Möglichkeit, die Aufbewahrungsrichtlinie für Amazon S3 S3-Buckets anzupassen, in denen Ihre AWS Control Tower CloudTrail Tower-Protokolle gespeichert werden. Sie können Ihre Amazon S3 S3-Richtlinie zur Aufbewahrung von Protokollen in Schritten von Tagen oder Jahren bis zu einem Maximum von 15 Jahren anpassen.

Wenn Sie Ihre Protokollaufbewahrung nicht anpassen möchten, sind die Standardeinstellungen 1 Jahr für die Standardkontenprotokollierung und 10 Jahre für die Zugriffsprotokollierung.

Diese Funktion ist für Bestandskunden über AWS Control Tower verfügbar, wenn Sie Ihre landing zone aktualisieren oder reparieren, und für Neukunden über den AWS Control Tower Tower-Setup-Prozess.

Reparatur von Role Drift verfügbar

11. August 2022

(Für die AWS Control Tower Tower-Landezone ist kein Update erforderlich.)

AWS Control Tower unterstützt jetzt die Reparatur von Rollenabweichungen. Sie können eine benötigte Rolle wiederherstellen, ohne Ihre landing zone vollständig reparieren zu müssen. Wenn diese Art von Drift-Reparatur erforderlich ist, finden Sie auf der Fehlerseite der Konsole 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 landing zone ist ein Update auf Version 3.0 erforderlich. Weitere Informationen finden Sie unterAktualisieren Ihrer Landing Zone)

Die AWS Control Tower landing zone Version 3.0 beinhaltet die folgenden Updates:

- Die Option, Trails auf Organisationsebene zu wählen oder sich von AWS CloudTrail CloudTrail Trails abzumelden, die von AWS Control Tower verwaltet werden.
- Zwei neue Detektivkontrollen, mit denen Sie feststellen können, 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 für die Region Deny Control.
- Eine Aktualisierung 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 seinen Kontopfad erstellt. Bei Organization Trails erstellen wir nur einen im Verwaltungskonto.

In den folgenden Abschnitten finden Sie weitere Informationen zu den einzelnen neuen Funktionen.

CloudTrail Trails auf Organisationsebene in AWS Control Tower

Mit landing zone Version 3.0 unterstützt AWS Control Tower jetzt Trails auf Organisationsebene AWS CloudTrail .

Wenn Sie Ihre AWS Control Tower-Landezone auf Version 3.0 aktualisieren, haben Sie die Möglichkeit, AWS CloudTrail Trails auf Organisationsebene als 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 nicht registrierte Konten. In dem unwahrscheinlichen Fall, dass Ihr landing zone 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 anfallen, bis Ihr Aktualisierungsvorgang erfolgreich abgeschlossen werden kann.

Ab landing zone 3.0 unterstützt AWS Control Tower keine verwalteten Trails auf Kontoebene mehr. 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 S3-Bucket verbleiben, in dem sie gespeichert werden. Nur die Trails werden gelöscht, nicht die vorhandenen Logs. Wenn Sie die Option zum Hinzufügen von Trails auf Organisationsebene auswählen, öffnet AWS Control Tower einen neuen Pfad zu einem neuen Ordner in Ihrem Amazon S3 S3-Bucket und sendet weiterhin Protokollierungsinformationen an diesen Speicherort. Wenn Sie sich dafür entscheiden, die von AWS Control Tower verwalteten Trails abzulehnen, bleiben Ihre vorhandenen Protokolle unverändert im Bucket.

Konventionen zur Benennung von Pfaden für den Protokollspeicher

- Konto-Trail-Logs werden mit einem Pfad in der folgenden Form gespeichert: `/org id/AWSLogs/…`
- Protokolldateien von Organisationen werden mit einem Pfad in der folgenden Form gespeichert: `/org id/AWSLogs/org id/…`

Der Pfad, den AWS Control Tower für Ihre CloudTrail Trails auf Organisationsebene erstellt, unterscheidet sich vom Standardpfad für einen manuell erstellten Trail auf Organisationsebene, der die folgende Form haben würde:

- `/AWSLogs/org id/…`

Weitere Informationen zur CloudTrail Pfadbenennung finden Sie unter Ihre Protokolldateien finden. CloudTrail

> **Tip**
>
> Wenn Sie planen, Ihre eigenen Trails auf Kontoebene zu erstellen und zu verwalten, empfehlen wir Ihnen, die neuen Trails zu erstellen, bevor Sie das Update auf AWS Control Tower landing zone Version 3.0 abschließen, um sofort mit der Protokollierung zu beginnen.

Sie können jederzeit neue CloudTrail Trails auf Konto- oder Organisationsebene erstellen und diese selbst verwalten. Die Option, CloudTrail Trails auf Organisationsebene auszuwählen, die von AWS Control Tower verwaltet werden, ist bei jedem landing zone Zone-Update auf Version 3.0 oder höher verfügbar. Du kannst Trails auf Organisationsebene aktivieren und deaktivieren, wann immer du deine landing zone aktualisierst.

Wenn Ihre Logs von einem Drittanbieter verwaltet werden, geben Sie Ihrem Dienst unbedingt den neuen Pfadnamen.

> **Note**
>
> Für Landezonen mit Version 3.0 oder höher werden AWS CloudTrail Trails auf Kontoebene von 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 von AWS Control Tower verwaltet werden.

Erfassen Sie AWS Config Ressourcen nur in der Heimatregion

In landing zone Version 3.0 hat AWS Control Tower die Basiskonfiguration für aktualisiert, AWS Config sodass globale Ressourcen nur 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 und empfohlen und ermöglicht 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 von einem Kunden oder einem AWS Service erstellt, aktualisiert oder gelöscht wurde, für jedes Element in jeder kontrollierten Region ein Konfigurationselement erstellt.

Zwei neue Detektivsteuerungen für die AWS CloudTrail Protokollierung

Im Rahmen der Umstellung auf AWS CloudTrail Trails auf Organisationsebene führt AWS Control Tower zwei neue Erkennungskontrollen ein, die überprüfen, ob sie aktiviert CloudTrail sind. Das erste Steuerelement verfügt über eine obligatorische Anleitung und ist auf der Security OU bei Setup- oder Landingzone-Updates von 3.0 und höher aktiviert. Für das zweite Steuerelement wird dringend empfohlen, und es wird optional auf alle Organisationseinheiten außer der Sicherheits-Organisationseinheit angewendet, für die der obligatorische Kontrollschutz bereits durchgesetzt ist.

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 Steuerungen finden Sie in der AWS Control Tower Controls Library.

Ein Update für die Region Deny Control

Wir haben die NotActionListe in der Region „Steuerung verweigern“ aktualisiert und enthält nun auch Aktionen einiger zusätzlicher Dienste, 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

In diesem Video (3:07) wird beschrieben, wie Sie Ihre bestehende AWS Control Tower Tower-Landing landing zone 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.

Exemplarische Videoanleitung zur Aktualisierung einer bestehenden AWS Control Tower Tower-Landing Zone auf Landing Zone 3.

Auf der Organisationsseite werden Ansichten von Organisationseinheiten und Konten zusammengefasst

18. Juli 2022

(Für die AWS Control Tower Tower-Landezone ist kein Update erforderlich)

Die neue Organisationsseite in AWS Control Tower zeigt eine hierarchische Ansicht aller Organisationseinheiten (OUs) und Konten. Sie kombiniert die Informationen aus den Seiten Organisationseinheiten und Konten, die zuvor vorhanden waren.

Auf der neuen Seite können Sie die Beziehungen zwischen übergeordneten Organisationseinheiten und ihren verschachtelten Organisationseinheiten und Konten sehen. Sie können Maßnahmen für Gruppierungen von Ressourcen ergreifen. Sie können die Seitenansicht konfigurieren. Sie können beispielsweise die hierarchische Ansicht erweitern oder reduzieren, die Ansicht filtern, sodass nur Konten oder Organisationseinheiten angezeigt werden, 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.

Einfachere Registrierung und Aktualisierung für einzelne Mitgliedskonten

31. Mai 2022

(Für die AWS Control Tower Tower-Landezone ist kein Update erforderlich)

AWS Control Tower bietet Ihnen jetzt eine verbesserte Möglichkeit, Mitgliedskonten einzeln zu aktualisieren und zu registrieren. Für jedes Konto wird angezeigt, wann es für ein Update verfügbar ist, sodass Sie leichter sicherstellen können, dass Ihre Mitgliedskonten die neueste Konfiguration enthalten. In wenigen einfachen Schritten können Sie Ihre landing zone aktualisieren, Kontoabweichungen beheben oder ein Konto für eine registrierte Organisationseinheit registrieren.

Wenn Sie ein Konto aktualisieren, müssen Sie nicht die gesamte Organisationseinheit (OU) eines Kontos in jede Aktualisierungsaktion einbeziehen. Dadurch wird der Zeitaufwand für die Aktualisierung eines einzelnen Kontos erheblich reduziert.

Mithilfe der AWS Control Tower Tower-Konsole können Sie Konten für AWS Control Tower Tower-Organisationseinheiten registrieren. Bestehende Konten, die Sie bei AWS Control Tower registrieren, müssen weiterhin die Kontovoraussetzungen erfüllen, und Sie müssen die `AWSControlTowerExecution` Rolle hinzufügen. Anschließend können Sie eine beliebige registrierte Organisationseinheit auswählen und das Konto dort registrieren, indem Sie auf die Schaltfläche „Registrieren“ klicken.

Wir haben die Funktion „Konto registrieren“ vom Workflow „Konto erstellen“ in Account Factory getrennt, um diese ähnlichen Prozesse besser voneinander zu unterscheiden und Einrichtungsfehler bei der Eingabe von Kontoinformationen zu vermeiden.

AFT unterstützt automatisierte Anpassungen für gemeinsam genutzte AWS Control Tower Tower-Konten

27. Mai 2022

(Für die AWS Control Tower 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 Prüfkontos und des Protokollarchiv-Kontos sowie Ihrer registrierten Konten. Sie können Ihre Kontoanpassung und das Aktualisierungsmanagement zentralisieren und gleichzeitig die Sicherheit Ihrer Kontokonfigurationen schützen, da Sie die Rolle, die die Arbeit ausführt, selbst festlegen.

Mit der vorhandenen AWSAFTExecutionRolle werden nun Anpassungen für alle Konten bereitgestellt. Sie können IAM-Berechtigungen mit Grenzen einrichten, die den Zugriff auf die

AWSAFTExecutionRolle 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 AWSAFTServiceRolle für die Bereitstellung von AFT-Ressourcen für alle verwalteten Konten, einschließlich der gemeinsamen Konten und des Verwaltungskontos. Ressourcen wurden früher von der AWSAFTExecutionRolle bereitgestellt.

Die gemeinsamen Konten und Verwaltungskonten von AWS Control Tower werden nicht über Account Factory bereitgestellt, sodass sie nicht über die entsprechenden bereitgestellten Produkte verfügen. AWS Service Catalog Daher können Sie die gemeinsamen Konten und Verwaltungskonten in Service Catalog nicht aktualisieren.

Gleichzeitige Operationen für alle optionalen Steuerelemente

18. Mai 2022

(Für die AWS Control Tower Tower-Landezone ist kein Update erforderlich)

AWS Control Tower unterstützt jetzt gleichzeitige Operationen für präventive Kontrollen sowie für detektive Kontrollen.

Mit dieser neuen Funktion kann jetzt jede optionale Steuerung 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 AWS Control Tower gerade dabei ist, eine landing zone einzurichten oder die Verwaltung auf eine neue Organisation auszudehnen.

Unterstützte Funktionen für präventive Kontrollen:

- Wenden Sie verschiedene präventive Kontrollen auf derselben Organisationseinheit an und entfernen Sie sie.
- Wenden Sie verschiedene präventive Kontrollen auf verschiedenen Organisationseinheiten gleichzeitig an und entfernen Sie sie.
- Wenden Sie dieselbe präventive Kontrolle auf mehrere Organisationseinheiten gleichzeitig an und entfernen Sie sie.

- Sie können alle präventiven und detektiven Kontrollen gleichzeitig anwenden und entfernen.

Sie können diese Verbesserungen der Parallelität bei der Steuerung 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-OU 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 Leitplanken 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 AWS Control Tower Tower-Steuerungsbibliothek.

Bestehende Sicherheits- und Protokollierungskonten

16. Mai 2022

(Bei der Ersteinrichtung verfügbar.)

AWS Control Tower bietet Ihnen jetzt die Möglichkeit, während der ersten Einrichtung der landing zone ein vorhandenes AWS Konto als AWS Control Tower Tower-Sicherheits- oder Protokollierungskonto anzugeben. Diese Option macht es überflüssig, dass AWS Control Tower neue, gemeinsame Konten erstellt. Das Sicherheitskonto, das standardmäßig als Auditkonto bezeichnet wird, ist ein eingeschränktes Konto, das Ihren Sicherheits- und Compliance-Teams Zugriff auf alle Konten in Ihrer landing zone gewährt. Das Protokollierungskonto, das standardmäßig als Log Archive-Konto bezeichnet wird, dient als Repository. Es speichert Protokolle von API-Aktivitäten und Ressourcenkonfigurationen von allen Konten in Ihrer landing zone.

Indem Sie Ihre bestehenden Sicherheits- und Protokollierungskonten verwenden, ist es einfacher, die AWS Control Tower-Governance auf Ihre bestehenden Organisationen auszudehnen oder von einer alternativen landing zone zu AWS Control Tower zu wechseln. Die Option, bestehende Konten zu verwenden, wird bei der ersten Einrichtung der landing zone angezeigt. Sie umfasst Prüfungen während des Einrichtungsprozesses, die eine erfolgreiche Bereitstellung sicherstellen. AWS Control Tower implementiert die erforderlichen Rollen und Kontrollen für Ihre bestehenden Konten. Es werden keine vorhandenen Ressourcen oder Daten, die in diesen Konten vorhanden sind, entfernt oder zusammengeführt.

Einschränkung: Wenn Sie planen, bestehende AWS Konten als Audit- und Protokollarchivkonten in 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-Landezone, Version 2.9

22. April 2022

(Für die AWS Control Tower landing zone ist ein Update auf Version 2.9 erforderlich. Weitere Informationen finden Sie unterAktualisieren Ihrer Landing Zone)

AWS Control Tower landing zone Version 2.9 aktualisiert den Notification Forwarder Lambda, sodass er die Python-Laufzeit der Version 3.9 verwendet. Dieses Update behebt die veraltete Version 3.6 von Python, die für Juli 2022 geplant ist. Die neuesten Informationen finden Sie auf der Python-Verfallsseite.

AWS-Control-Tower-Landezone, Version 2.8

10. Februar 2022

(Für die AWS Control Tower landing zone ist ein Update auf Version 2.8 erforderlich. Weitere Informationen finden Sie unterAktualisieren Ihrer Landing Zone)

Die AWS Control Tower landing zone Version 2.8 fügt Funktionen hinzu, die den jüngsten Aktualisierungen der Best Practices für AWS grundlegende 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-Zugriffs-Log-Bucket nachzuverfolgen.
- Support für Lebenszyklusrichtlinien wurde hinzugefügt. Das Zugriffsprotokoll für den vorhandenen S3-Zugriffsprotokoll-Bucket ist auf eine standardmäßige Aufbewahrungszeit von 10 Jahren festgelegt.
- Darüber hinaus aktualisiert diese Version AWS Control Tower so, dass es die von AWS Config bereitgestellte AWS Service Linked Role (SLR) in allen verwalteten Konten (mit Ausnahme des Verwaltungskontos) verwendet, sodass Sie Config-Regeln einrichten und verwalten können, die den AWS Config Best Practices entsprechen. Kunden, die kein Upgrade durchführen, werden weiterhin ihre bestehende Rolle verwenden.

- 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 enthält ein Update für die Region Deny Control, um die `route53-application-recovery` Funktion in zu ermöglichen. `us-west-2`
- Update: Am 15. Februar 2022 haben wir die Warteschlange für tote Buchstaben für AWS Lambda-Funktionen entfernt.

Weitere Details:

- Wenn Sie Ihre landing zone nehmen, entfernt AWS Control Tower die AWS Config serviceverknüpfte Rolle nicht.
- Wenn Sie die Bereitstellung eines Account Factory Factory-Kontos aufheben, entfernt AWS Control Tower die AWS Config serviceverknüpfte Rolle nicht.

Um Ihre landing zone auf 2.8 zu aktualisieren, navigieren Sie zur Seite mit den Landingzone-Einstellungen, wählen Sie die Version 2.8 aus und wählen Sie dann Aktualisieren. Nachdem Sie Ihre landing zone aktualisiert haben, müssen Sie alle Konten aktualisieren, die von AWS Control Tower verwaltet werden, wie unter beschriebenVerwaltung von Konfigurationsupdates in AWS Control Tower.

Januar bis Dezember 2021

Im Jahr 2021 veröffentlichte AWS Control Tower die folgenden Updates:

- Region verweigert Funktionen
- Funktionen zur Datenresidenz
- AWS Control Tower führt die Bereitstellung und Anpassung von Terraform-Konten ein
- Neues Lebenszyklus-Ereignis verfügbar
- AWS Control Tower ermöglicht verschachtelte Organisationseinheiten
- Parallelität mit detektivischer Kontrolle
- Zwei neue Regionen verfügbar
- Abwahl der Region
- AWS Control Tower arbeitet mit AWS Schlüsselverwaltungssystemen

- Steuerung umbenannt, Funktionalität unverändert
- AWS Control Tower scannt SCPs täglich, um zu prüfen, ob Abweichungen vorliegen
- Benutzerdefinierte Namen für Organisationseinheiten und Konten
- AWS-Control-Tower-Landezone, Version 2.7
- Drei neue AWS Regionen verfügbar
- Regiert nur ausgewählte Regionen
- AWS Control Tower erweitert jetzt die Governance auf bestehende Organisationseinheiten in Ihren AWS Organisationen
- AWS Control Tower bietet Bulk-Kontoaktualisierungen

Region verweigert Funktionen

30. November 2021

(Für die AWS Control Tower Tower-Landezone ist kein Update erforderlich.)

AWS Control Tower bietet jetzt Region-Deny-Funktionen, mit denen Sie den Zugriff auf AWS Services und Operationen für registrierte Konten in Ihrer AWS Control Tower Tower-Umgebung einschränken können. Die Funktion Region verweigern ergänzt die bestehenden Funktionen zur Regionsauswahl und zur Abwahl von Regionen in AWS Control Tower. Zusammen helfen Ihnen diese Funktionen dabei, Bedenken im Zusammenhang mit der Einhaltung gesetzlicher Vorschriften und Vorschriften auszuräumen 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 von AWS Control Tower oder auf der Seite mit den Landingzone-Einstellungen auswählen. Die Funktion Region Deny ist verfügbar, wenn Sie Ihre AWS Control Tower Tower-Landing Zone-Version aktualisieren. Ausgewählte AWS Services sind von der Funktion „Region Deny“ ausgenommen. Weitere Informationen finden Sie unter Konfiguration der Steuerung „Regionsverweigerung“.

Funktionen zur Datenresidenz

30. November 2021

(Für die AWS Control Tower Tower-Landezone ist kein Update erforderlich)

AWS Control Tower bietet jetzt speziell entwickelte Kontrollen, um sicherzustellen, dass sich alle Kundendaten, die Sie in AWS Services hochladen, nur in den von Ihnen angegebenen AWS 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 Kontrolle können Sie zusätzliche Kontrollen anwenden, z. B. Amazon Virtual Private Network (VPN) -Verbindungen verbieten oder den Internetzugang für eine Amazon VPC-Instance verbieten. Sie können den Compliance-Status der Kontrollen in der AWS Control Tower Tower-Konsole einsehen. Eine vollständige Liste der verfügbaren Steuerelemente finden Sie in der AWS Control Tower Tower-Steuerungsbibliothek.

AWS Control Tower führt die Bereitstellung und Anpassung von Terraform-Konten ein

29. November 2021

(Optionales Update für die AWS Control Tower 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-Infrastructure-as-Code-Pipeline (IaC), die Konten bereitstellt, die von AWS Control Tower verwaltet werden. Anpassungen während der Bereitstellung tragen dazu bei, 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, wodurch zusätzliche Terraform-Module ausgelöst werden, 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 alle AFT-Funktionsoptionen hinzufügen möchten, die von für allgemeine Anpassungen bereitgestellt werden. AWS

Beginnen Sie mit AWS Control Tower Account Factory for Terraform, indem Sie die Schritte im AWS Control Tower Tower-Benutzerhandbuch befolgen und AFT für Ihre Terraform-Instance

herunterladen. Stellen Sie AWS Control Tower Account Factory für Terraform (AFT) bereit AFT unterstützt die Open-Source-Distributionen Terraform Cloud, Terraform Enterprise und Terraform.

Neues Lebenszyklus-Ereignis verfügbar

18. November 2021

(Für die AWS Control Tower Tower-Landezone ist kein Update erforderlich)

Das `PrecheckOrganizationalUnit` Ereignis protokolliert, ob Ressourcen, einschließlich Ressourcen in verschachtelten Organisationseinheiten, den Erfolg der Aufgabe „Steuerung erweitern“ verhindern. Weitere Informationen finden Sie unter `PrecheckOrganizationalUnit`.

AWS Control Tower ermöglicht verschachtelte Organisationseinheiten

16. November 2021

(Für die AWS Control Tower Tower-Landezone ist kein Update erforderlich)

Mit AWS Control Tower können Sie jetzt verschachtelte Organisationseinheiten als Teil Ihrer landing zone einbeziehen.

AWS Control Tower bietet Unterstützung für verschachtelte Organisationseinheiten (OUs), sodass Sie Konten in mehreren Hierarchieebenen organisieren und präventive Kontrollen hierarchisch durchsetzen können. Sie können Organisationseinheiten registrieren, die verschachtelte Organisationseinheiten enthalten, Organisationseinheiten unter übergeordneten Organisationseinheiten erstellen und registrieren und Kontrollen für jede registrierte Organisationseinheit aktivieren, unabhängig von deren Umfang. Um diese Funktionalität zu unterstützen, zeigt die Konsole die Anzahl der verwalteten Konten und Organisationseinheiten an.

Mit verschachtelten Organisationseinheiten können Sie Ihre AWS Control Tower Tower-Organisationseinheiten an der Strategie für AWS mehrere Konten ausrichten und den Zeitaufwand für die Aktivierung von Kontrollen für mehrere Organisationseinheiten reduzieren, indem Sie Kontrollen auf der Ebene der übergeordneten Organisationseinheit durchsetzen.

Die wichtigsten Überlegungen

1. Sie können bestehende, mehrstufige OUs bei AWS Control Tower registrieren, eine OU nach der anderen, wobei Sie mit der Organisationseinheit der obersten Ebene beginnen und dann die Struktur nach unten fortsetzen. Weitere Informationen finden Sie unter Erweitern Sie von einer flachen OU-Struktur zu einer verschachtelten OU-Struktur.

2. Konten, die direkt einer registrierten Organisationseinheit unterstehen, werden automatisch registriert. Konten, die weiter unten in der Liste stehen, können registriert werden, indem die ihnen unmittelbar übergeordnete Organisationseinheit registriert wird.
3. Präventive Kontrollen (SCPs) werden automatisch nach unten in der Hierarchie vererbt. SCPs, die auf die übergeordnete Organisationseinheit angewendet werden, werden von allen verschachtelten Organisationseinheiten übernommen.
4. Detective Controls (AWS Config-Regeln) werden NICHT automatisch vererbt.
5. Die Einhaltung der Detective Controls wird von jeder Organisationseinheit gemeldet.
6. Die Änderung des SCP-Werts auf einer Organisationseinheit wirkt sich auf alle Konten und Organisationseinheiten aus, die ihr unterstehen.
7. Sie können unter der Sicherheits-OU (Core-OU) keine neuen verschachtelten OUs erstellen.

Parallelität mit detektivischer Kontrolle

5. November 2021

(Optionales Update für die AWS Control Tower Tower-Landezone)

AWS Control Tower Detective Controls unterstützen jetzt gleichzeitige Operationen für detektive Kontrollen und verbessern so die Benutzerfreundlichkeit und Leistung. Sie können mehrere Detective Controls aktivieren, ohne auf den Abschluss einzelner Kontrollvorgänge warten zu müssen.

Unterstützte Funktionen:

- Aktivieren Sie verschiedene Detective Controls auf derselben Organisationseinheit (z. B. „Erkennen, ob MFA für den Root-Benutzer aktiviert ist“ und „Erkennen, ob öffentlicher Schreibzugriff auf Amazon S3 S3-Buckets zulässig ist“).
- Aktivieren Sie gleichzeitig verschiedene Detective Controls für verschiedene Organisationseinheiten.
- Die Guardrail-Fehlermeldungen wurden verbessert und bieten nun zusätzliche Hinweise zu unterstützten Parallelitätsoperationen.

In dieser Version nicht unterstützt:

- Die gleichzeitige Aktivierung derselben Detective Control für mehrere Organisationseinheiten wird nicht unterstützt.

- Die gleichzeitige Nutzung der präventiven Kontrolle wird nicht unterstützt.

Sie können die Verbesserungen der Parallelität von Detective Control in allen Versionen von AWS Control Tower erleben. Es wird empfohlen, dass Kunden, die derzeit nicht Version 2.7 verwenden, ein landing zone Zone-Update durchführen, um andere Funktionen wie die Auswahl und Abwahl von Regionen nutzen zu können, die in der neuesten Version verfügbar sind.

Zwei neue Regionen verfügbar

29. Juli 2021

(Update für die AWS Control Tower Tower-Landezone erforderlich)

AWS Control Tower ist jetzt in zwei weiteren AWS Regionen verfügbar: Südamerika (Sao Paulo) und Europa (Paris). Mit diesem Update wird die Verfügbarkeit von AWS Control Tower auf 15 AWS Regionen erweitert.

Wenn Sie neu bei AWS Control Tower sind, 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 die Seite Landing Zone Settings in Ihrem AWS Control Tower Tower-Dashboard auf und wählen Sie dann die Regionen aus. Nachdem Sie Ihre landing zone aktualisiert haben, müssen Sie anschließend alle Konten aktualisieren, die von AWS Control Tower verwaltet werden.

Abwahl der Region

29. Juli 2021

(Optionales Update für die AWS Control Tower Tower-Landezone)

Wenn Sie die AWS-Control-Tower-Region abwählen, können Sie die geografische Präsenz Ihrer AWS Control Tower Tower-Ressourcen besser verwalten. Sie können die Auswahl von Regionen aufheben, für die AWS Control Tower nicht mehr zuständig sein soll. Diese Funktion bietet Ihnen die Möglichkeit, Bedenken im Zusammenhang mit der Einhaltung gesetzlicher Vorschriften und Vorschriften auszuräumen und gleichzeitig die mit der Expansion in weitere Regionen verbundenen Kosten auszugleichen.

Die Abwahl der Region ist verfügbar, wenn Sie Ihre AWS Control Tower 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 Kontrolle — in den von Ihnen ausgewählten Regionen in den Konten bereit. Wenn Sie sich dafür entscheiden, eine Region abzuwählen und AWS Control Tower Governance aus dieser Region zu entfernen, wird diese Governance-Funktionalität entfernt, aber Ihre Benutzer können dadurch nicht daran gehindert werden, AWS Ressourcen oder Workloads in diesen Regionen bereitzustellen.

AWS Control Tower arbeitet mit AWS Schlüsselverwaltungssystemen

28. Juli 2021

(Optionales Update für die AWS Control Tower 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 Services, einschließlich AWS CloudTrail, und der zugehörigen Amazon S3 S3-Daten AWS Config, zu sichern. AWS Die KMS-Verschlüsselung ist eine erweiterte Verschlüsselungsstufe gegenüber der SSE-S3-Verschlüsselung, die AWS Control Tower standardmäßig verwendet.

Die Integration der AWS KMS-Unterstützung in AWS Control Tower entspricht den bewährten Methoden der AWS Grundlagensicherheit, die eine zusätzliche Sicherheitsebene für Ihre sensiblen 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 Tower-Landing landing zone aktualisieren.

Um diese Funktionalität zu konfigurieren, können Sie bei der ersten Einrichtung der landing zone die Option 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 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 AWS Control Tower Tower-Landezone ist kein Update erforderlich)

AWS Control Tower überarbeitet derzeit die Namen und Beschreibungen bestimmter Kontrollen, um die politischen Absichten der Kontrolle besser widerzuspiegeln. Die überarbeiteten Namen und Beschreibungen helfen Ihnen dabei, intuitiver zu verstehen, wie Kontrollen die Richtlinien Ihrer Konten verkörpern. Wir haben zum Beispiel einen Teil der Namen der detektiven Kontrollen von „Nicht zulassen“ in „Erkennen“ geändert, da die detektive Kontrolle selbst keine bestimmte Aktion unterbindet, sondern nur Richtlinienverstöße erkennt und über das Dashboard Warnmeldungen ausgibt.

Die Kontrollfunktion, die Anleitung und die Implementierung bleiben unverändert. Lediglich die Namen und Beschreibungen der Steuerelemente wurden überarbeitet.

AWS Control Tower scannt SCPs täglich, um zu prüfen, ob Abweichungen vorliegen

11. Mai 2021

(Für die AWS Control Tower Tower-Landezone ist kein Update erforderlich)

AWS Control Tower führt jetzt täglich automatische Scans Ihrer verwalteten SCPs durch, um zu überprüfen, ob die entsprechenden Kontrollen korrekt angewendet wurden und ob sie nicht verändert wurden. Wenn bei einem 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.

Benutzerdefinierte Namen für Organisationseinheiten und Konten

16. April 2021

(Für die AWS Control Tower Tower-Landezone ist kein Update erforderlich)

Mit AWS Control Tower können Sie jetzt die Benennung Ihrer landing zone anpassen. Sie können die Namen beibehalten, die AWS Control Tower für die Organisationseinheiten (OUs) und Kernkonten empfiehlt, oder Sie können diese Namen während der ersten Einrichtung der landing zone ändern.

Die Standardnamen, die AWS Control Tower für die Organisationseinheiten und Kernkonten bereitstellt, entsprechen den Best Practices-Richtlinien für AWS mehrere Konten. Wenn Ihr Unternehmen jedoch spezifische Benennungsrichtlinien hat oder wenn Sie bereits eine Organisationseinheit oder ein Konto mit demselben empfohlenen Namen haben, bietet Ihnen die neue Funktion zur Benennung von Organisationseinheiten und Konten die Flexibilität, diese Einschränkungen zu berücksichtigen.

Unabhängig von dieser Änderung des Workflows während der Einrichtung wird die Organisationseinheit, die früher als Core-OU bekannt war, jetzt als Sicherheits-OU bezeichnet, und die Organisationseinheit, die früher als benutzerdefinierte Organisationseinheit bekannt war, wird jetzt als Sandbox-OU bezeichnet. Wir haben diese Änderung vorgenommen, um uns besser an die allgemeinen AWS Best-Practice-Leitlinien für die Benennung anzupassen.

Neue Kunden werden diese neuen OU-Namen sehen. Bestandskunden werden weiterhin die ursprünglichen Namen dieser Organisationseinheiten sehen. Während wir unsere Dokumentation an die neuen Namen anpassen, kann es zu Unstimmigkeiten bei der Benennung der Organisationseinheiten kommen.

Um mit AWS Control Tower von der AWS Management Console aus zu beginnen, gehen Sie zur AWS Control Tower Tower-Konsole und wählen Sie oben rechts landing zone einrichten aus. Weitere Informationen finden Sie unter Planung Ihrer AWS Control Tower Tower-Landezone.

AWS-Control-Tower-Landezone, Version 2.7

8. April 2021

(Für die AWS Control Tower landing zone ist ein Update auf Version 2.7 erforderlich. Weitere Informationen finden Sie unterAktualisieren Ihrer Landing Zone)

Mit AWS Control Tower Version 2.7 führt AWS Control Tower vier neue obligatorische präventive Protokollarchive-Kontrollen ein, mit denen Richtlinien ausschließlich auf AWS Control Tower Tower-Ressourcen implementiert werden. Wir haben die Leitlinien für vier bestehende Log Archive-Kontrollen von verpflichtend auf fakultativ angepasst, da sie Richtlinien für Ressourcen außerhalb von AWS Control Tower festlegen. Diese Änderung und Erweiterung der Steuerung bietet die Möglichkeit, die Verwaltung des Protokollarchivs für Ressourcen innerhalb von AWS Control Tower von der Verwaltung von Ressourcen außerhalb von AWS Control Tower zu trennen.

Die vier geänderten Kontrollen können in Verbindung mit den neuen obligatorischen Kontrollen verwendet werden, um die Verwaltung eines breiteren Spektrums von AWS Protokollarchiven zu gewährleisten. In bestehenden AWS Control Tower Tower-Umgebungen bleiben diese vier

geänderten Kontrollen aus Gründen der Umgebungskonsistenz automatisch aktiviert. Diese optionalen Kontrollen können jetzt jedoch deaktiviert werden. Neue AWS Control Tower Tower-Umgebungen müssen alle optionalen Kontrollen ermöglichen. Bestehende Umgebungen müssen die zuvor obligatorischen Kontrollen deaktivieren, bevor Amazon S3 S3-Buckets, die nicht von AWS Control Tower bereitgestellt werden, verschlüsselt werden.

Neue obligatorische Kontrollen:

- Änderungen an der Verschlüsselungskonfiguration für von AWS Control Tower erstellte S3-Buckets im Protokollarchiv nicht zulassen
- Änderungen an der Protokollierungskonfiguration für von AWS Control Tower erstellte S3-Buckets im Protokollarchiv nicht zulassen
- Änderungen an der Bucket-Richtlinie für von AWS Control Tower erstellte S3-Buckets im Protokollarchiv nicht zulassen
- Änderungen an der Lebenszykluskonfiguration für von AWS Control Tower erstellte S3-Buckets im Protokollarchiv nicht zulassen

Die Beratung wurde von Pflicht zu Wahlfach geändert:

- Änderungen an der Verschlüsselungskonfiguration für alle Amazon S3 S3-Buckets nicht zulassen [Bisher: Encryption at Rest for Log Archive aktivieren]
- Änderungen an der Protokollierungskonfiguration für alle Amazon S3 S3-Buckets nicht zulassen [Bisher: Zugriffsprotokollierung für Log Archive aktivieren]
- Änderungen an der Bucket-Richtlinie für alle Amazon S3 S3-Buckets nicht zulassen [Bisher: Richtlinienänderungen im Protokollarchiv nicht zulassen]
- Änderungen an der Lebenszykluskonfiguration für alle Amazon S3 S3-Buckets nicht zulassen [Bisher: Eine Aufbewahrungsrichtlinie für das Protokollarchiv festlegen]

AWS Control Tower Version 2.7 beinhaltet Änderungen am AWS Control Tower landing zone Zone-Blueprint, die nach dem Upgrade auf 2.7 zu Inkompatibilität mit früheren Versionen führen können.

- Insbesondere wird AWS Control Tower Version 2.7 `BlockPublicAccess` automatisch für S3-Buckets aktiviert, die von AWS Control Tower bereitgestellt werden. Sie können diese Standardeinstellung deaktivieren, wenn für Ihren Workload ein kontenübergreifender Zugriff erforderlich ist. Weitere Informationen darüber, was mit `Blockpublicaccess` aktivierter Option passiert, finden Sie unter Sperren des öffentlichen Zugriffs auf Ihren Amazon S3 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 durch diese Änderung die Fehlermeldung „Zugriff verweigert“, was möglicherweise Ihren Arbeitsablauf beeinträchtigen kann. Diese Änderung kann nach dem Update 2.7 für deine landing zone nicht mehr rückgängig gemacht werden.

  Wir empfehlen Ihnen, Ihre Anfragen so zu ändern, dass sie TLS statt HTTP verwenden.

Drei neue AWS Regionen verfügbar

8. April 2021

(Update für die AWS Control Tower Tower-Landezone erforderlich)

AWS Control Tower ist in drei weiteren AWS Regionen verfügbar: Asien-Pazifik (Tokio), Region Asien-Pazifik (Seoul) und Region Asien-Pazifik (Mumbai). Für die Ausweitung der Verwaltung auf diese Regionen ist ein landing zone Zone-Update auf Version 2.7 erforderlich.

Ihre landing zone wird nicht automatisch auf diese Regionen ausgedehnt, wenn Sie das Update auf Version 2.7 durchführen. Sie müssen sie in der Tabelle Regionen anzeigen und auswählen, damit sie aufgenommen werden können.

Regiert nur ausgewählte Regionen

19. Februar 2021

(Für die AWS Control Tower Tower-Landezone ist kein Update erforderlich)

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.

Die Regionsauswahl ist verfügbar, wenn Sie eine neue landing zone einrichten oder Ihre AWS Control Tower Tower-Landingzone-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 Kontrolle 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 Tower-Regionen

AWS Control Tower erweitert jetzt die Governance auf bestehende Organisationseinheiten in Ihren AWS Organisationen

28. Januar 2021

(Für die AWS Control Tower Tower-Landezone ist kein Update erforderlich)

Erweitern Sie die Steuerung von der AWS Control Tower-Konsole aus auf bestehende Organisationseinheiten (OUs) (die sich nicht in AWS Control Tower befinden). Mit dieser Funktion können Sie Organisationseinheiten der obersten Ebene und die darin enthaltenen Konten unter die Kontrolle von AWS Control Tower stellen. Informationen zur Ausweitung der Governance auf eine gesamte Organisationseinheit 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 Verwaltung und Registrierung von Konten innerhalb der OU erfolgreich verlängert wird. Weitere Informationen zu häufig auftretenden Problemen im Zusammenhang mit der Erstregistrierung einer Organisationseinheit finden Sie unter. Häufige Ursachen für Fehler bei der Registrierung oder Neuregistrierung

Sie können auch die AWS Control Tower-Produktwebseite besuchen oder YouTube sich dieses Video über die ersten Schritte mit AWS Control Tower for ansehen AWS Organizations.

AWS Control Tower bietet Bulk-Kontoaktualisierungen

28. Januar 2021

(Für die AWS Control Tower Tower-Landezone ist kein Update erforderlich)

Mit der Funktion für Massenaktualisierungen 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 Tower-Dashboard aktualisieren. Dies ist besonders nützlich, wenn Sie Ihre AWS Control Tower Tower-Landezone aktualisieren und auch Ihre registrierten Konten aktualisieren müssen, um sie an die aktuelle Landingzone-Version anzupassen.

Diese Funktion hilft Ihnen auch dabei, Ihre Konten auf dem neuesten Stand zu halten, wenn Sie Ihre AWS Control Tower Tower-Landing landing zone aktualisieren, um sie auf neue Regionen auszudehnen, oder wenn Sie eine Organisationseinheit erneut registrieren möchten, um sicherzustellen, dass für alle Konten in dieser Organisationseinheit die neuesten Kontrollen angewendet werden. Durch die Aktualisierung mehrerer Konten entfällt die Notwendigkeit, jeweils ein Konto zu aktualisieren oder ein externes Skript zu verwenden, um die Aktualisierung für mehrere Konten durchzuführen.

Hinweise zum Aktualisieren einer landing zone finden Sie unterAktualisieren Ihrer Landing Zone.

Informationen 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 Tower-Konsole ist jetzt mit externen AWS Konfigurationsregeln verknüpft
- AWS Control Tower jetzt in weiteren Regionen verfügbar
- Aktualisierung von Guardrail
- Die AWS Control Tower Tower-Konsole zeigt mehr Details zu OUs und Konten
- Verwenden Sie AWS Control Tower, um neue AWS Umgebungen mit mehreren Konten einzurichten in AWS Organizations
- Anpassungen für die AWS Control Tower Tower-Lösung
- Allgemeine Verfügbarkeit von AWS Control Tower Version 2.3
- Kontobereitstellung in einem Schritt in AWS Control Tower
- Tool zur Außerbetriebnahme von AWS Control Tower
- Benachrichtigungen zu Ereignissen im Lebenszyklus von AWS Control Tower

Die AWS Control Tower Tower-Konsole ist jetzt mit externen AWS Konfigurationsregeln verknüpft

29. Dezember 2020

(Für die AWS Control Tower landing zone ist ein Update auf Version 2.6 erforderlich. Weitere Informationen finden Sie unterAktualisieren Ihrer Landing Zone)

AWS Control Tower umfasst jetzt einen Aggregator auf Organisationsebene, der bei der Erkennung externer AWS Konfigurationsregeln hilft. Auf diese Weise können Sie in der AWS Control Tower-Konsole sehen, ob es zusätzlich zu den von AWS Control Tower erstellten AWS AWS Config-Regeln auch extern erstellte Config-Regeln gibt. Der Aggregator ermöglicht es AWS Control Tower, externe Regeln zu erkennen und einen Link zur AWS Config-Konsole bereitzustellen, ohne dass AWS Control Tower Zugriff auf nicht verwaltete Konten erhalten muss.

Mit dieser Funktion haben Sie jetzt einen konsolidierten Überblick über die auf Ihre Konten angewandten Detektivkontrollen, 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 jetzt in weiteren Regionen verfügbar

18. November 2020

(Für die AWS Control Tower landing zone ist ein Update auf Version 2.5 erforderlich. Weitere Informationen finden Sie unterAktualisieren Ihrer 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 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. Weitere Informationen finden Sie unter Konfigurieren Sie Ihre AWS Control Tower Tower-Regionen.

Aktualisierung von Guardrail

8. Oktober 2020

(Für die AWS Control Tower Tower-Landezone 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 Änderungen an von AWS Control Tower AWS eingerichteten IAM-Rollen nicht zulassen und AWS CloudFormation im Referenzhandbuch zu AWS Control Tower Controls.

Die AWS Control Tower Tower-Konsole zeigt mehr Details zu OUs und Konten

22. Juli 2020

(Für die AWS Control Tower Tower-Landezone ist kein Update erforderlich)

Sie können Ihre Organisationen und Konten, die nicht bei AWS Control Tower registriert sind, sowie Organisationen und Konten, die registriert sind, einsehen.

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.

Verwenden Sie AWS Control Tower, um neue AWS Umgebungen mit mehreren Konten einzurichten in AWS Organizations

22. April 2020

(Für die AWS Control Tower Tower-Landezone 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 landing zone für neue Organisationseinheiten (OUs) einrichten. Sie können neue Organisationseinheiten in AWS Control Tower und neue Konten in diesen Organisationseinheiten mit AWS Control Tower Tower-Governance erstellen.
- AWS Organizations Kunden können bestehende Konten mithilfe des Kontoregistrierungsprozesses oder mithilfe von Skripten registrieren.

AWS Control Tower bietet einen Orchestrierungsservice, der andere AWS Services verwendet. Es wurde für Unternehmen 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 von AWS Control Tower verwaltet wird, wissen Cloud-Administratoren, dass die Konten in der Organisation den festgelegten Richtlinien entsprechen. Bauherren profitieren davon, dass sie schnell neue AWS Konten einrichten können, ohne sich Sorgen um die Einhaltung der Vorschriften machen zu müssen.

Informationen zum Einrichten einer landing zone finden Sie unterPlanen Ihrer Landing Zone von AWS Control Tower. Sie können auch die AWS Control Tower-Produktwebseite besuchen oder YouTube sich dieses Video über die ersten Schritte mit AWS Control Tower for ansehen AWS Organizations.

Zusätzlich zu dieser Änderung wurde die Funktion zur schnellen Kontobereitstellung in 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 bestehendes Konto.

Anpassungen für die AWS Control Tower Tower-Lösung

17. März 2020

(Für die AWS Control Tower Tower-Landezone 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 Tower-Landezone anwenden können.

Mit Anpassungen für AWS Control Tower können Sie AWS CloudFormation Vorlagen verwenden, um neue Ressourcen für bestehende und neue Konten in Ihrem Unternehmen bereitzustellen. Sie können zusätzlich zu den bereits von AWS Control Tower bereitgestellten SCPs auch benutzerdefinierte Service Control Policies (SCPs) auf diese Konten anwenden. Anpassungen für die AWS Control Tower-Pipeline lassen sich mit Ereignissen und Benachrichtigungen (Lebenszyklusereignisse in AWS Control Tower) im Lebenszyklus von AWS Control Tower integrieren, um sicherzustellen, dass die Ressourcenbereitstellungen mit Ihrer landing zone synchron bleiben.

Die Bereitstellungsdokumentation für diese AWS Control Tower Tower-Lösungsarchitektur ist auf der AWS Solutions-Webseite verfügbar.

Allgemeine Verfügbarkeit von AWS Control Tower Version 2.3

5. März 2020

(Update für die AWS Control Tower Tower-Landezone erforderlich. Weitere Informationen finden Sie unterAktualisieren Ihrer Landing Zone.)

AWS Control Tower ist jetzt in der AWS Region Asien-Pazifik (Sydney) zusätzlich zu 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 AWS Control Tower noch nicht verwendet haben, können Sie es heute in jeder der unterstützten Regionen starten. Wenn Sie AWS Control Tower bereits verwenden und dessen Governance-Funktionen in Ihren Konten auf die Region Asien-Pazifik (Sydney) ausweiten möchten, rufen Sie die Seite Einstellungen in Ihrem AWS Control Tower Tower-Dashboard auf. Aktualisieren Sie von dort aus Ihre landing zone auf die neueste Version. Aktualisieren Sie dann Ihre Konten einzeln.

> **Note**
>
> Durch die Aktualisierung Ihrer landing zone werden Ihre Konten nicht automatisch aktualisiert. Wenn Sie mehr als ein paar Konten haben, können die erforderlichen Aktualisierungen zeitaufwändig sein. Aus diesem Grund empfehlen wir Ihnen, Ihre AWS Control Tower 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 Konfiguration Ihrer AWS Control Tower Tower-Regionen.

Kontobereitstellung in einem Schritt in AWS Control Tower

2. März 2020

(Für die AWS Control Tower Tower-Landezone ist kein Update erforderlich)

AWS Control Tower unterstützt jetzt die Kontobereitstellung in einem Schritt über die AWS Control Tower Tower-Konsole. Mit dieser Funktion können Sie neue Konten von der AWS Control Tower Tower-Konsole aus einrichten.

Um das vereinfachte Formular zu verwenden, navigieren Sie in der AWS Control Tower Tower-Konsole zu Account Factory und wählen Sie dann Quick Account Provisioning. 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 mithilfe von Quick Account Provisioning 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 Tower-Konsole zu erstellen und zu aktualisieren, von der Möglichkeit, AWS Konten zu registrieren, getrennt. Weitere Informationen finden Sie unter Registrieren Sie ein bestehendes Konto.

Tool zur Außerbetriebnahme von AWS Control Tower

28. Februar 2020

(Für die AWS Control Tower Tower-Landezone ist kein Update erforderlich)

AWS Control Tower unterstützt jetzt ein automatisiertes Tool zur Außerbetriebnahme, das Sie bei der Bereinigung der von AWS Control Tower zugewiesenen Ressourcen unterstützt. 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 bereinigen, die bei der ersten Einrichtung Ihrer landing zone erstellt wurden.

Wenn Sie Ihre landing zone mithilfe eines weitgehend automatisierten Prozesses außer Betrieb nehmen möchten, wenden Sie sich an uns, AWS Support um Unterstützung bei den zusätzlichen erforderlichen Schritten zu erhalten. Weitere Informationen zur Außerbetriebnahme finden Sie unter. Exemplarische Vorgehensweise: Außerbetriebnahme einer AWS Control Tower Tower-Landezone

Benachrichtigungen zu Ereignissen im Lebenszyklus von AWS Control Tower

22. Januar 2020

(Für die AWS Control Tower Tower-Landezone 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 ändern kann, die von AWS Control Tower erstellt und verwaltet werden. Lebenszyklusereignisse 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 Steuerung 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 Services, um eine Best AWS Practices-Umgebung mit mehreren Konten aufzubauen und zu verwalten. Es kann mehrere Minuten dauern, bis eine AWS Control Tower Tower-Aktion abgeschlossen ist. Sie können Lebenszyklusereignisse in den CloudTrail Protokollen verfolgen, um zu überprüfen, ob die ursprüngliche AWS Control Tower 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 Automatisierungs-Workflow auszulösen.

Januar — Dezember 2019

Vom 1. Januar bis 31. Dezember 2019 veröffentlichte AWS Control Tower die folgenden Updates:

- Allgemeine Verfügbarkeit von AWS Control Tower Version 2.2
- Neue Wahlkontrollen in AWS Control Tower
- Neue Detektivkontrollen in AWS Control Tower
- AWS Control Tower akzeptiert E-Mail-Adressen für gemeinsam genutzte Konten mit anderen Domänen als dem Verwaltungskonto
- Allgemeine Verfügbarkeit von AWS Control Tower Version 2.1

Allgemeine Verfügbarkeit von AWS Control Tower Version 2.2

13. November 2019

(Update für die AWS Control Tower Tower-Landezone erforderlich. Weitere Informationen finden Sie unterAktualisieren Ihrer Landing Zone.)

AWS Control Tower, Version 2.2, bietet drei neue präventive Kontrollen, die eine Kontoabweichung verhindern:

- Änderungen an Amazon CloudWatch Logs-Protokollgruppen, die von AWS Control Tower eingerichtet wurden, nicht zulassen
- Löschen von AWS Config Aggregationsautorisierungen verbieten, die von AWS Control Tower erstellt wurden
- Löschen des Protokollarchivs nicht zulassen

Bei einer Kontrolle handelt es sich um eine Regel auf hoher Ebene, die eine kontinuierliche Steuerung Ihrer gesamten AWS Umgebung gewährleistet. Wenn Sie Ihre AWS Control Tower Tower-Landezone 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 (versehentlichen oder vorsätzlichen) Änderungen an diesem Compliance-Status kommen. Die Erkennung von Abweichungen hilft Ihnen dabei, Ressourcen zu identifizieren, die Änderungen oder Konfigurationsupdates benötigen, um die Abweichung zu beheben. Weitere Informationen finden Sie unter Abweichungen im AWS Control Tower erkennen und beheben.

Neue Wahlkontrollen in AWS Control Tower

05. September 2019

(Für die AWS Control Tower Tower-Landezone ist kein Update erforderlich)

AWS Control Tower umfasst jetzt die folgenden vier neuen Wahlkontrollen:

- Löschaktionen in Amazon S3 S3-Buckets ohne MFA nicht zulassen
- Änderungen an der Replikationskonfiguration für Amazon S3 S3-Buckets nicht zulassen
- Aktionen als Root-Benutzer verbieten
- Die Erstellung von Zugriffsschlüsseln für den Root-Benutzer verbieten

Bei einer Kontrolle handelt es sich um eine Regel auf hoher Ebene, die eine kontinuierliche Steuerung Ihrer gesamten AWS Umgebung gewährleistet. Leitlinien ermöglichen es Ihnen, Ihre Richtlinienziele auszudrücken. Weitere Informationen finden Sie unter Über Kontrollen in AWS Control Tower.

Neue Detektivkontrollen in AWS Control Tower

25. August 2019

(Für die AWS Control Tower Tower-Landezone ist kein Update erforderlich)

AWS Control Tower umfasst jetzt die folgenden acht neuen Detective Controls:

- Ermitteln Sie, ob die Versionierung für Amazon S3 S3-Buckets aktiviert ist
- Ermitteln Sie, ob MFA für IAM-Benutzer der Konsole aktiviert ist AWS
- Ermitteln Sie, ob MFA für IAM-Benutzer aktiviert ist
- Ermitteln Sie, ob die Amazon EBS-Optimierung für Amazon EC2 EC2-Instances aktiviert ist
- Ermitteln Sie, ob Amazon EBS-Volumes an Amazon EC2 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 Regel auf hoher Ebene, die eine kontinuierliche Steuerung Ihrer gesamten AWS Umgebung gewährleistet. Eine detektivische Kontrolle erkennt Verstöße gegen die Einhaltung der Vorschriften durch Ressourcen in Ihren Konten, z. B. Verstöße gegen Richtlinien, und gibt über das Dashboard Warnmeldungen aus. Weitere Informationen finden Sie unter Über Kontrollen in AWS Control Tower.

AWS Control Tower akzeptiert E-Mail-Adressen für gemeinsam genutzte Konten mit anderen Domänen als dem Verwaltungskonto

01. August 2019

(Für die AWS Control Tower Tower-Landezone ist kein Update erforderlich)

In AWS Control Tower können Sie jetzt E-Mail-Adressen für gemeinsame Konten (Protokollarchiv und Audit-Mitglied) und Kinderkonten (verkauft mit Account Factory) angeben, deren Domains sich von der E-Mail-Adresse des Verwaltungskontos unterscheiden. Diese Funktion ist nur verfügbar, wenn Sie eine neue landing zone erstellen und wenn Sie neue Kinderkonten einrichten.

Allgemeine Verfügbarkeit von AWS Control Tower Version 2.1

24. Juni 2019

(Update für die AWS Control Tower Tower-Landezone erforderlich. Weitere Informationen finden Sie unter Aktualisieren Sie Ihre Landezone.)

AWS Control Tower ist jetzt allgemein verfügbar und wird für den Produktionseinsatz unterstützt. AWS Control Tower richtet sich an Unternehmen 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.

Mit AWS Control Tower können Sie eine landing zone einrichten, in der bewährte Methoden wie die Konfiguration einer Struktur mit mehreren Konten, die Verwaltung von Benutzeridentitäten und Verbundzugriff mit AWS Organizations AWS IAM Identity Center, die Aktivierung der Kontobereitstellung über Service Catalog und die Erstellung eines zentralen Protokollarchivs mit und angewendet werden. AWS CloudTrail AWS Config

Für eine kontinuierliche Steuerung können Sie vorkonfigurierte Kontrollen aktivieren, bei denen es sich um klar definierte Regeln für Sicherheit, Betrieb und Compliance handelt. Leitplanken helfen dabei, den Einsatz von Ressourcen zu verhindern, die nicht den Richtlinien entsprechen, und überwachen die eingesetzten Ressourcen kontinuierlich auf Nichtkonformität. Das AWS Control Tower Tower-Dashboard bietet einen zentralen Einblick in eine AWS Umgebung, einschließlich bereitgestellter Konten, aktivierter Kontrollen und des Compliance-Status von Konten.

Sie können eine neue Umgebung mit mehreren Konten mit einem einzigen Klick in der AWS Control Tower Tower-Konsole einrichten. Für die Nutzung von AWS Control Tower fallen keine zusätzlichen Gebühren oder Vorabverpflichtungen an. Sie zahlen nur für die AWS Dienste, die Sie für die Einrichtung einer landing zone und die Implementierung ausgewählter Steuerungen aktiviert haben.

Dokumentverlauf

- Letzte Aktualisierung der Dokumentation: 20. Mai 2024

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
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 Steuerungen wurde in ein neues Handbuch verschoben	AWS Control Tower hat den Controls Reference Guide veröffentlicht.	21. April 2024
`EnabledControl` Ressourcen taggen in AWS CloudFormation	AWS Control Tower unterstützt das Hinzufügen von Tags zu `EnabledControl` Ressourcen mithilfe von AWS CloudFormation Vorlagen.	22. Februar 2024
Basis-APIs verfügbar	AWS Control Tower hat neue APIs für die programmgesteuerte 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.	8. 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 vertrauenswürdigen Zugriffs	AWS Control Tower benachrichtigt Kunden, wenn Abweichungen auftreten, 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-pazifischen 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 Hub-Detektivkontrollen verfügbar	AWS Control Tower erweitert die Kontrollbibliothek um zehn neue Kontrollen für den Security Hub 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	Unterstützung für Terraform-Open-Source-Blueprints in AFC in einer einzigen Region.	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 servicebezogene Rolle und AWSServiceRoleForAWSControlTowerdie zugehörige Richtlinie hinzugefügt. AWSControlTowerAccountServiceRolePolicy	01. Juni 2023
Update zur gemischten Verwaltung	Update, um Kunden in Bezug auf gemischte Unternehmensführung zu informieren.	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 AWSControlTowerServiceRolePolicy so 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 IAM-Methoden.	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 AWS 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 Steuerungen, Ressourcen AWS CloudFormation	AWS Control Tower unterstützt jetzt die Aktivierung und Deaktivierung von Kontrollen über eine Reihe von API-Aufrufen und eine neue AWS 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 Organisationsseite 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 AWSContro lTowerServiceRolePolicyso geändert, dass Kunden über AWS CloudTrail Trails auf Organisationsebene verfügen können, um Logs zu aggregier en AWS CloudTrail .	20. Juni 2022
Einfachere Registrierung und Aktualisierung von Mitglieds konten	AWS Control Tower bietet Ihnen jetzt die Möglichkeit, Mitgliedskonten einzeln von Ihrer landing zone aus zu registrieren und zu aktualisi eren. 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 unterstüt zt 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 Protokollkonten 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.